

ALSO Training – Fortinet Security Fabric

13./14.06.2017, Zurich, Renens, Emmen

Gabriel Kälin, Channel Systems Engineer

gkaelin@fortinet.com, +41 79 882 80 98

What You Can Learn in this Training

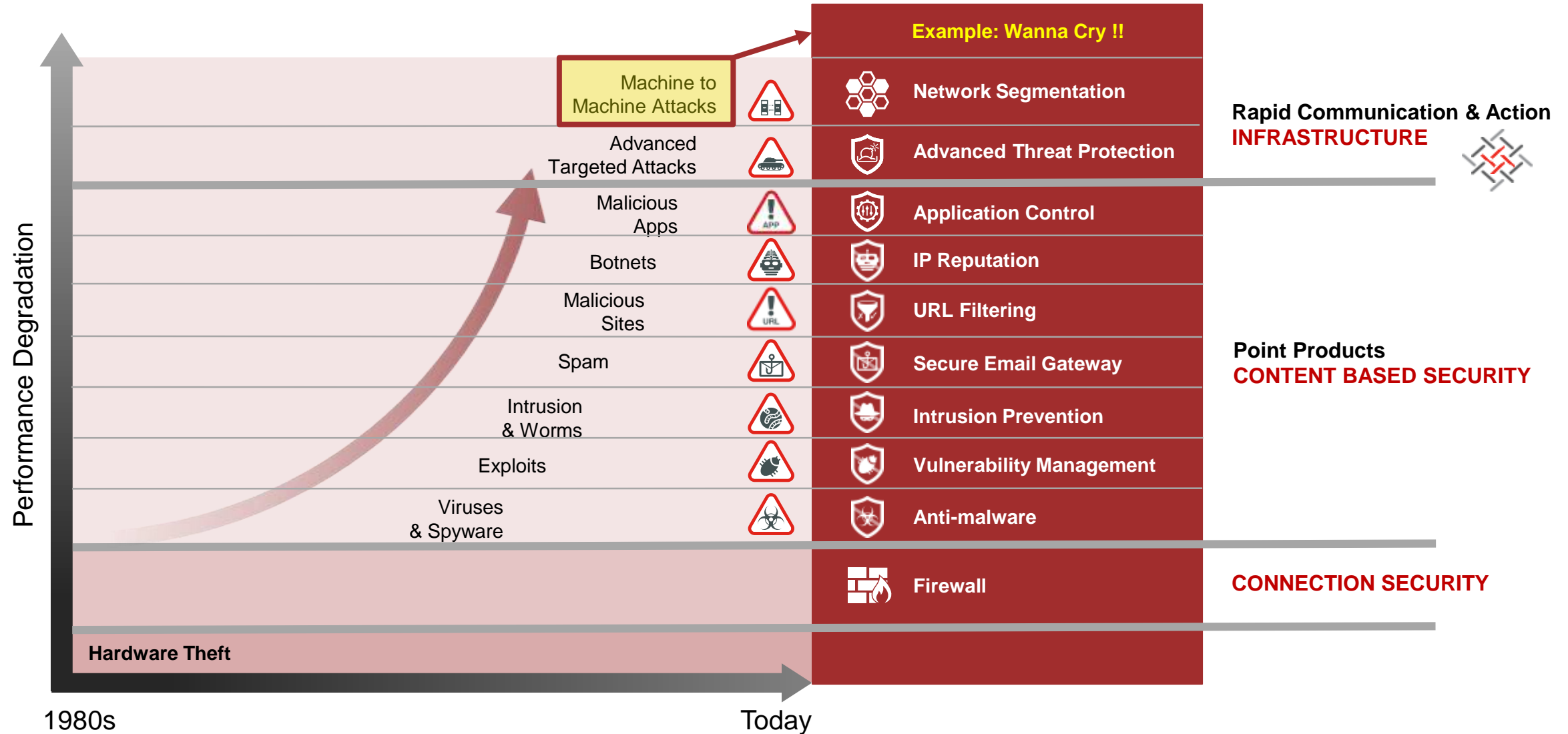
- Security Fabric Vision
 - Tight mesh of interconnected security controls
- Broad solution
 - Be informed about your environment, regardless what it looks like
 - Demo FortiView
- Powerful solution
 - Don't let security be an inhibitor, but an enabler
 - Security Fabric Audit demo
- Automated solution – profit to the max
 - Coordinated Advanced Threat Protection – demo
 - Go beyond FortiWorld



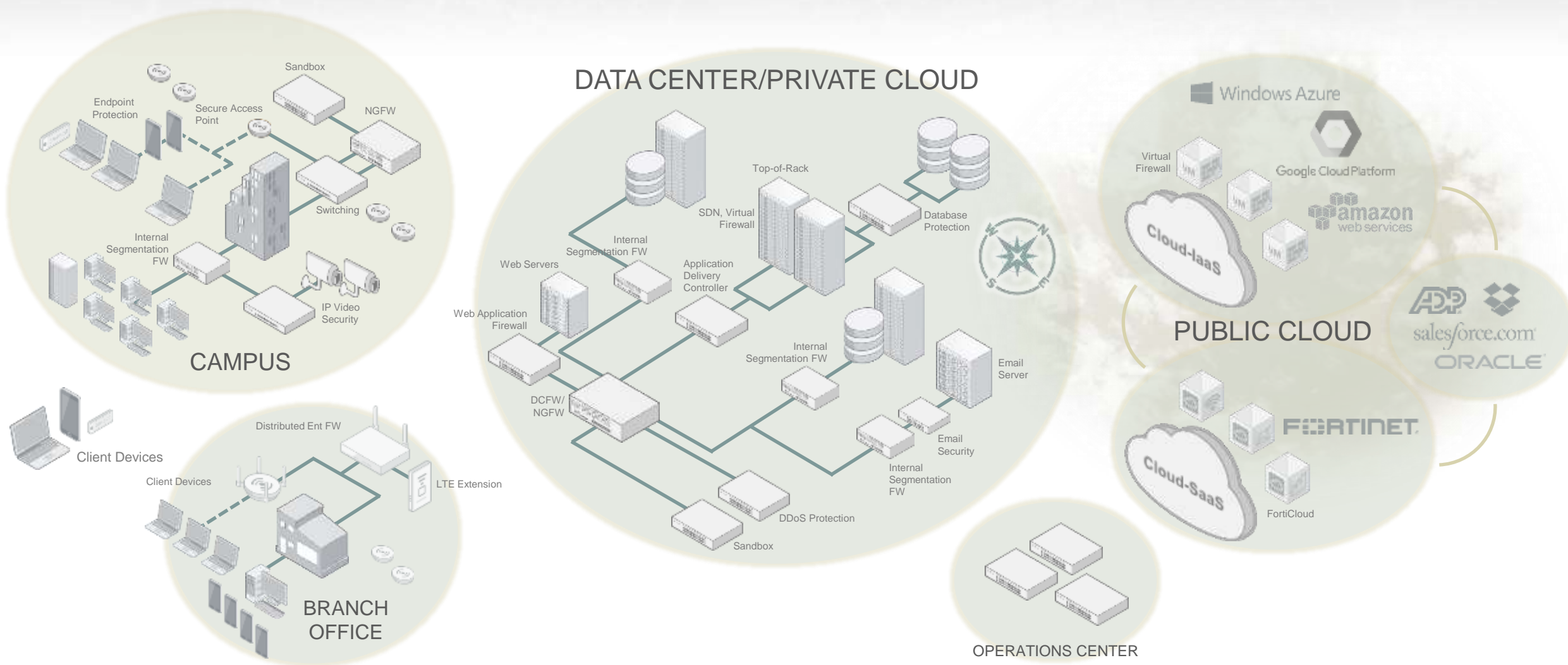
The Vision: Fortinet Security Fabric

Address today's threats with a tight mesh of interconnected security controls

The Threat and Performance Challenge Timeline



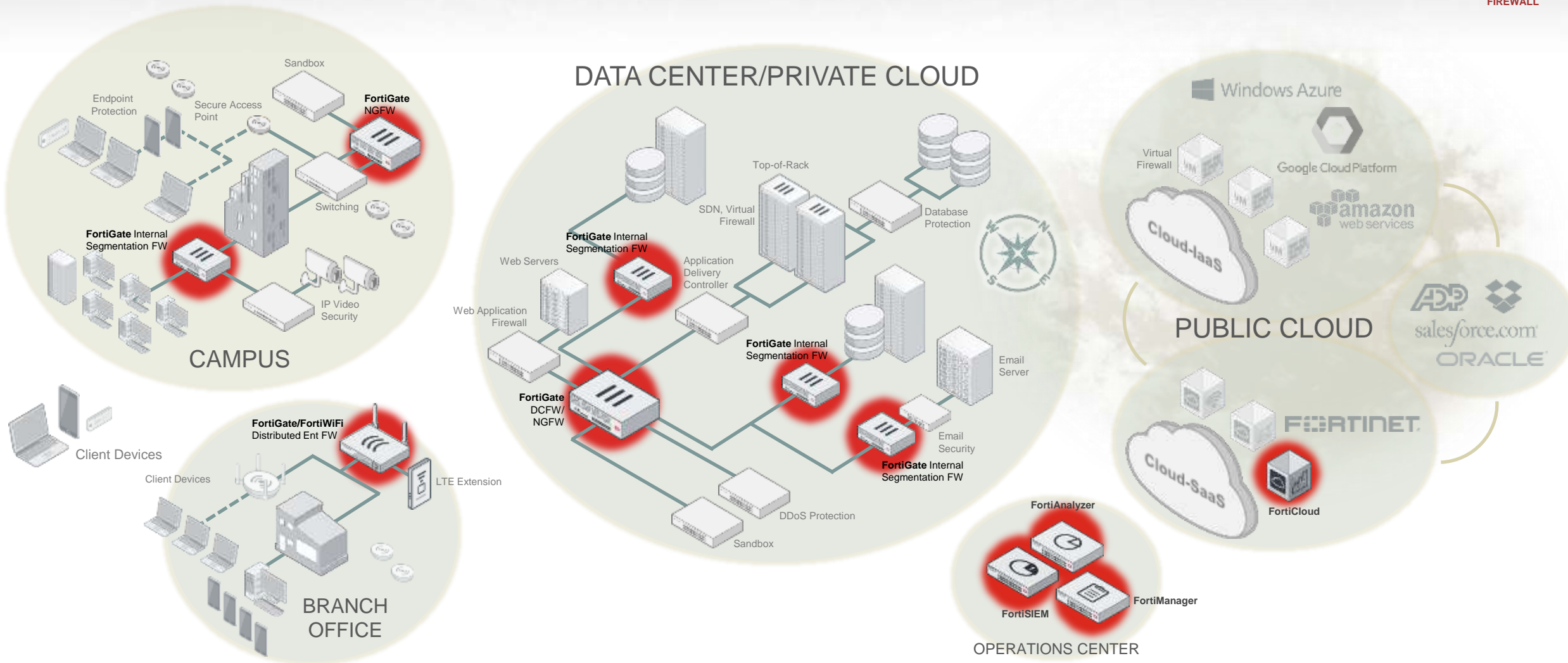
A Typical Enterprise Deployment Today



It All Starts with Fortinet Enterprise Firewalls



ENTERPRISE
FIREWALL



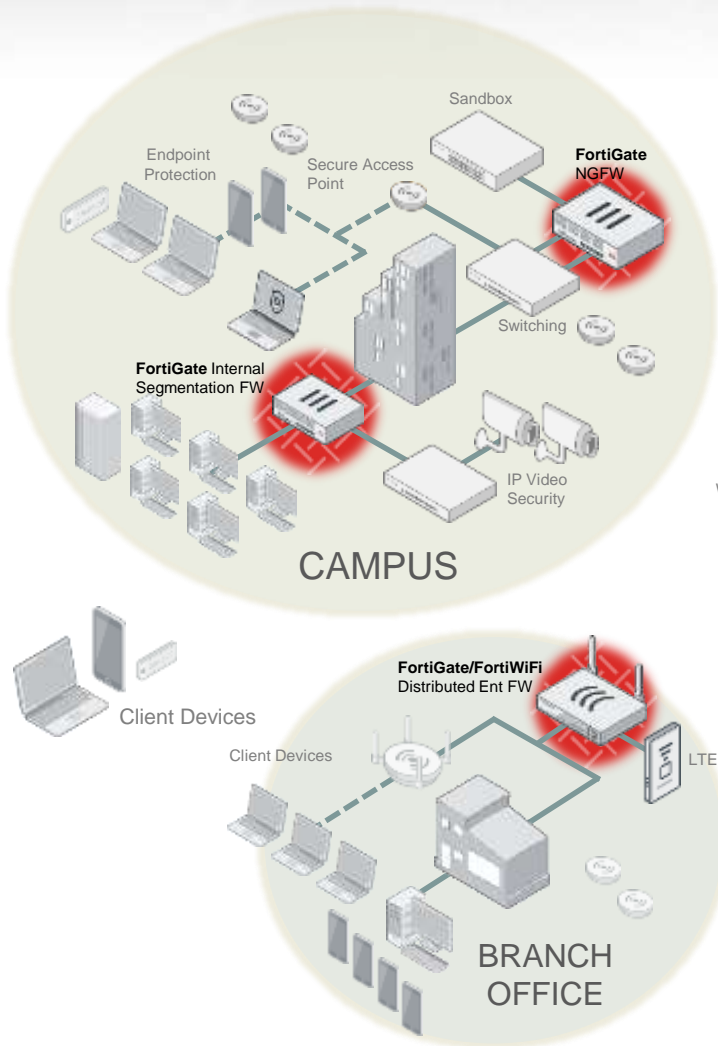
Regardless of Location or Form Factor



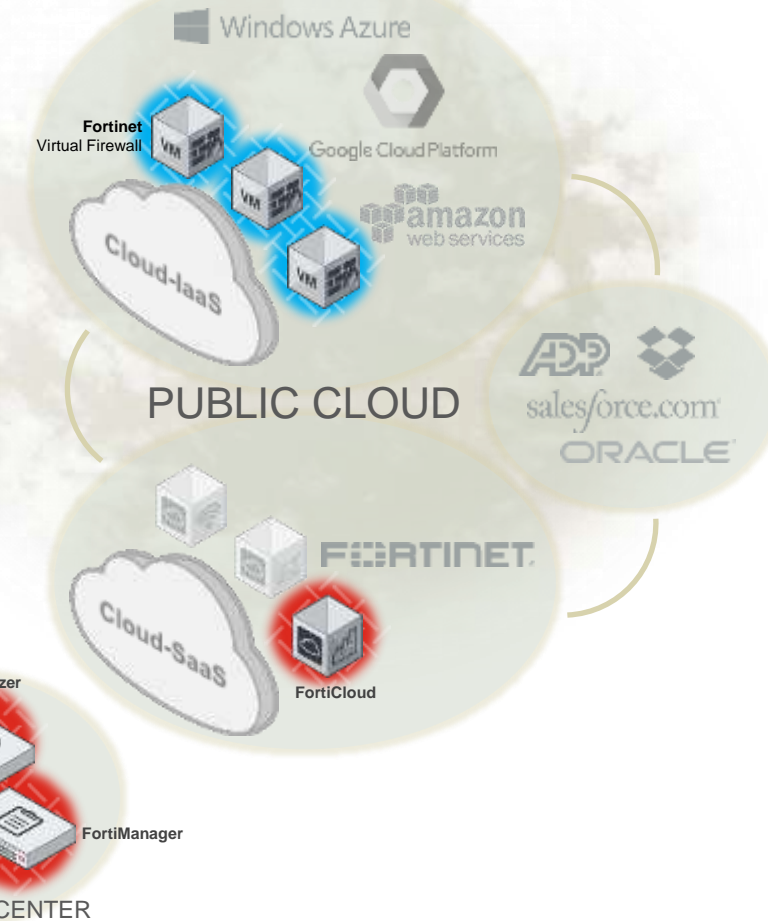
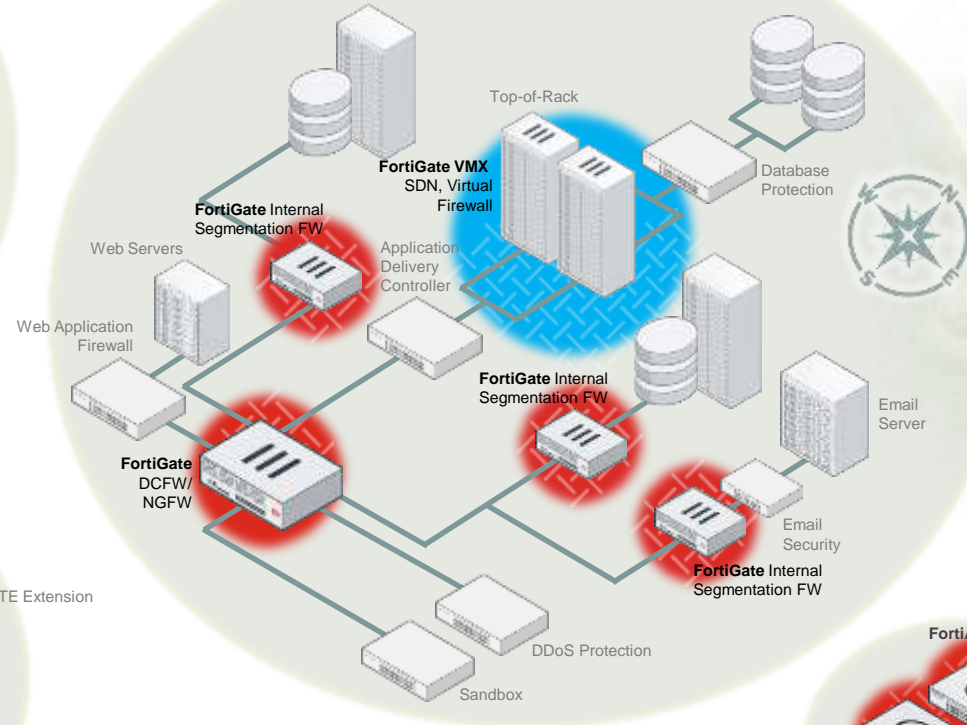
CLOUD SECURITY



ENTERPRISE
FIREWALL



DATA CENTER/PRIVATE CLOUD



Local Threat Intelligence with the ATP Solution



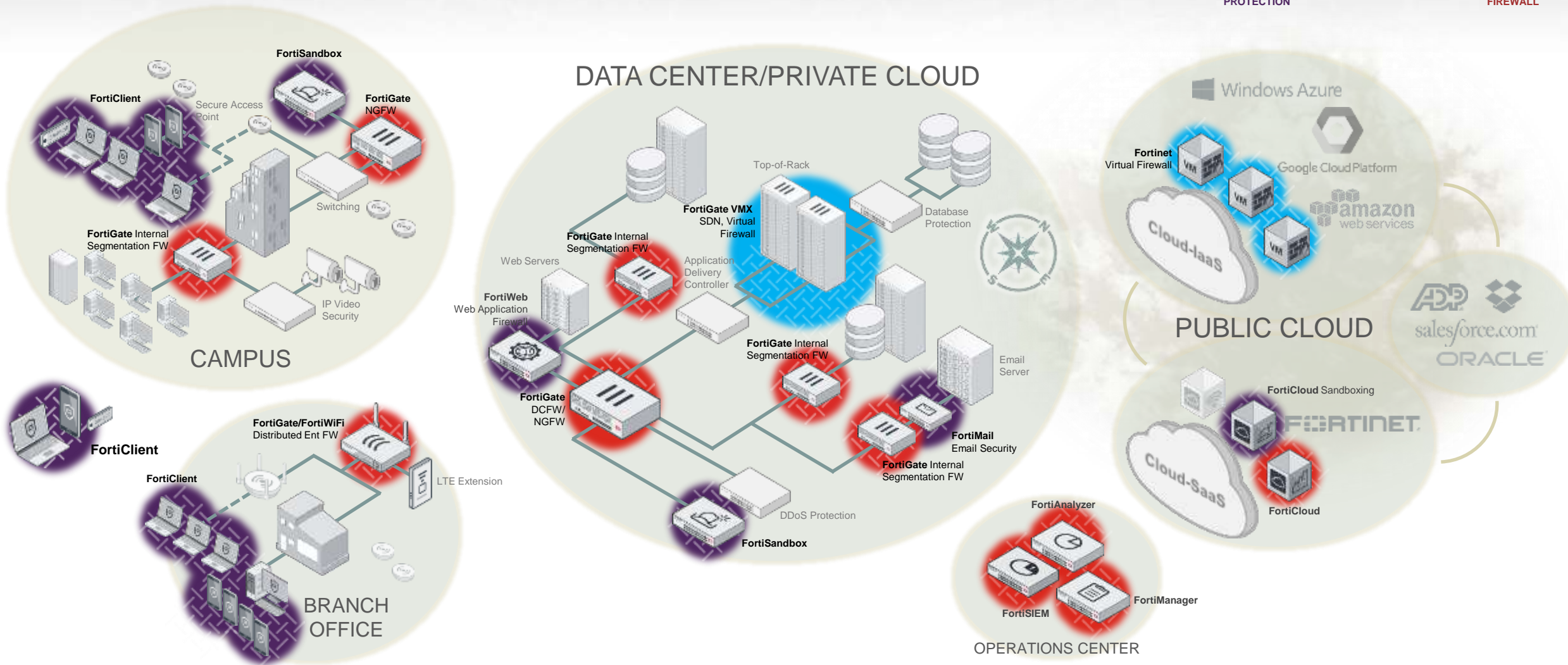
ADVANCED THREAT
PROTECTION



CLOUD SECURITY



ENTERPRISE
FIREWALL



Including the Application Layer



APPLICATION
SECURITY



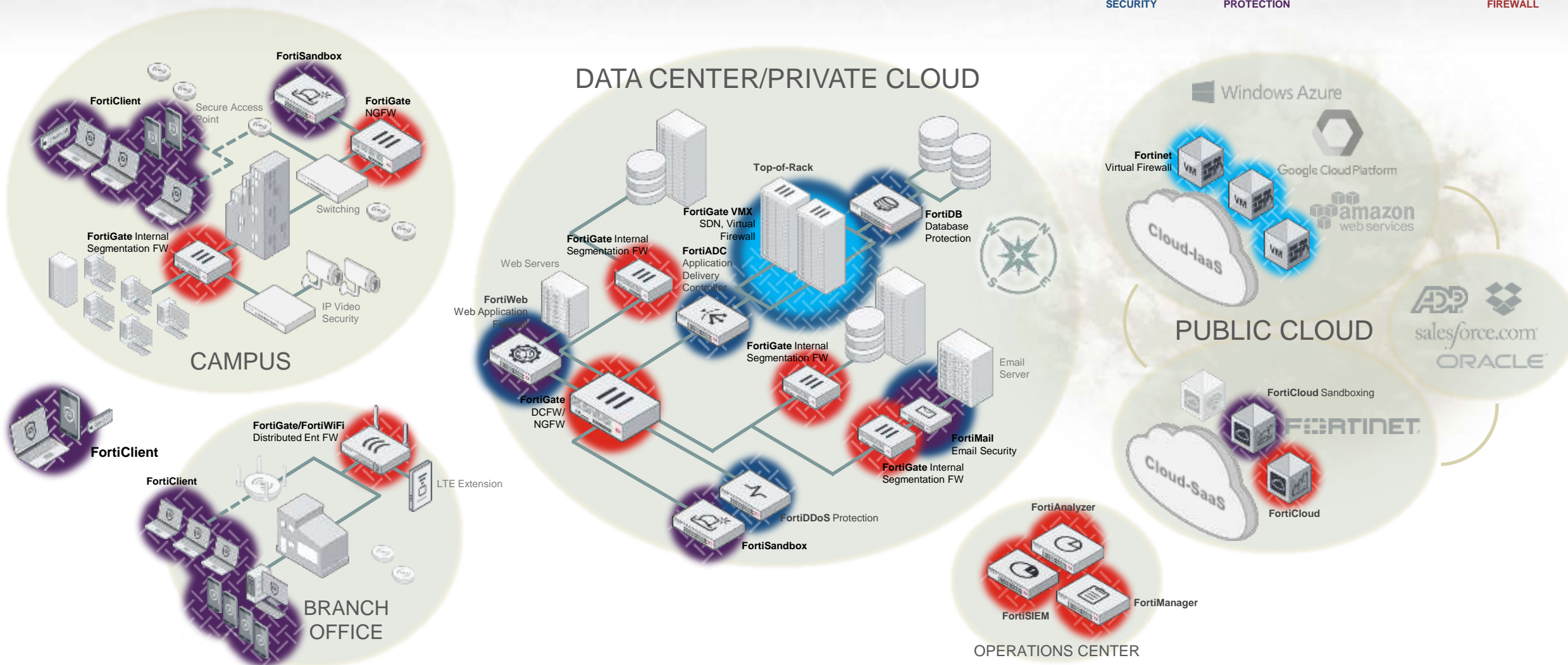
ADVANCED THREAT
PROTECTION



CLOUD SECURITY



ENTERPRISE
FIREWALL



... and the Endpoint and Access Infrastructure



SECURE ACCESS



APPLICATION
SECURITY



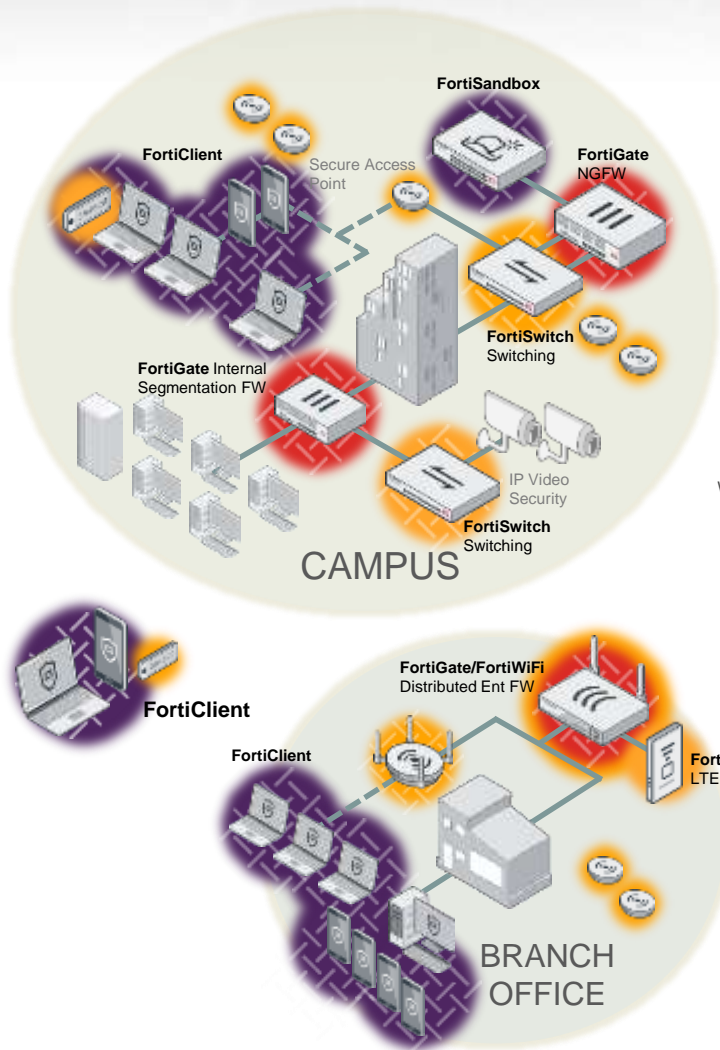
ADVANCED THREAT
PROTECTION



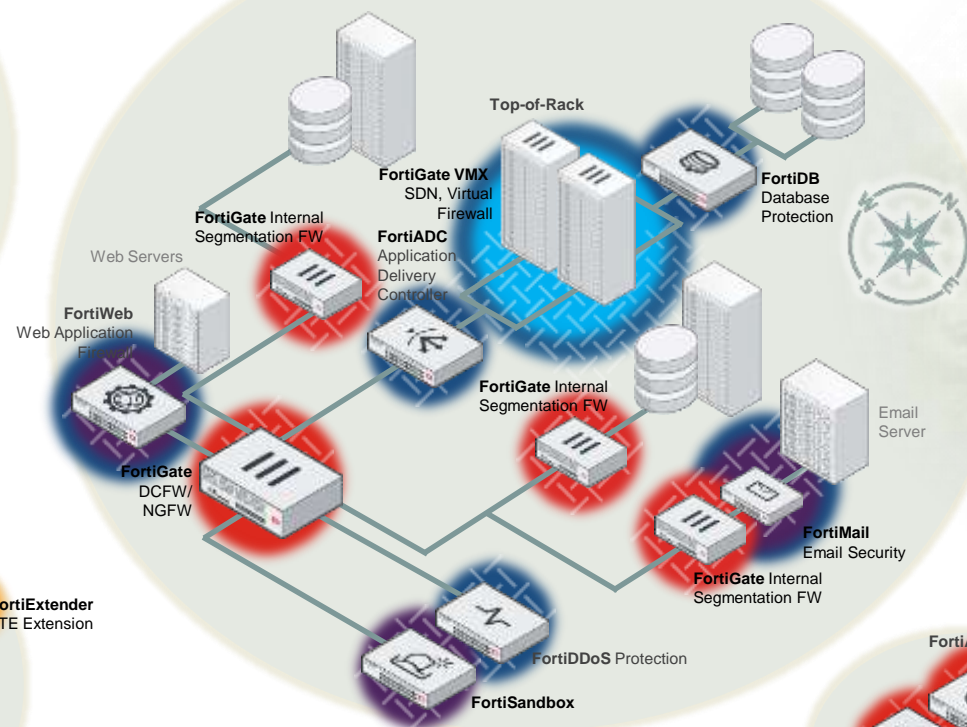
CLOUD SECURITY



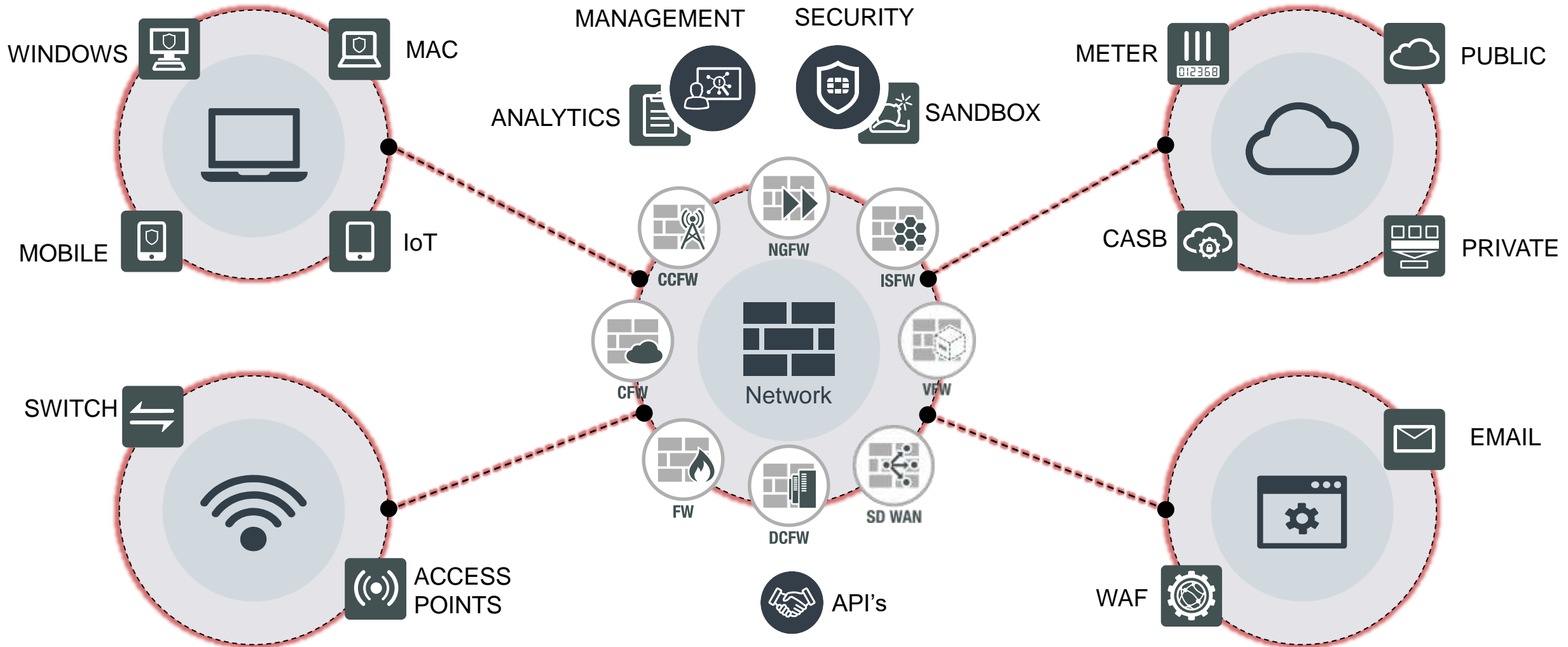
ENTERPRISE
FIREWALL



DATA CENTER/PRIVATE CLOUD






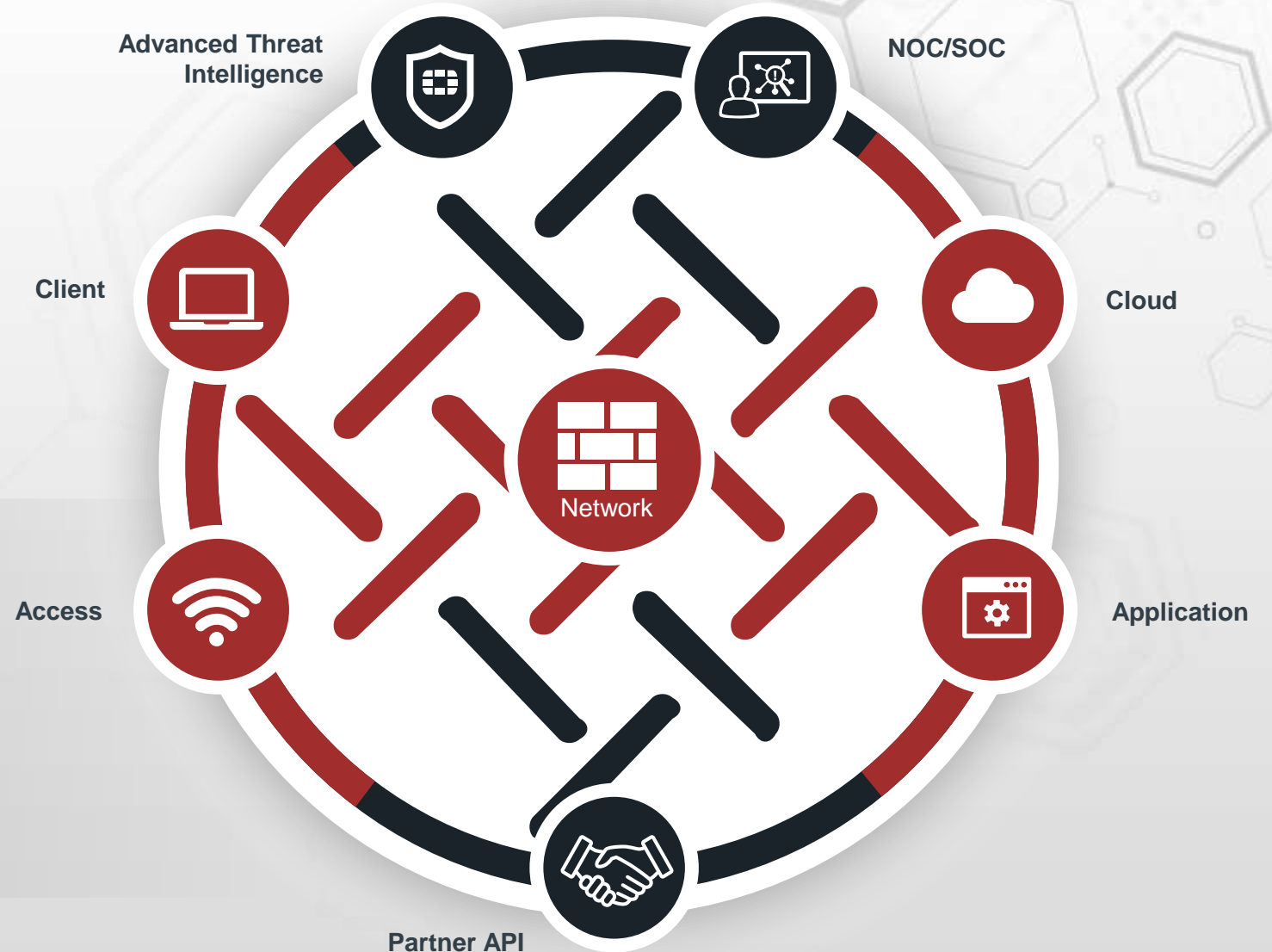
Span of the Security Fabric





The Fortinet Security Fabric is the vision that delivers on the promise of Security without Compromise:

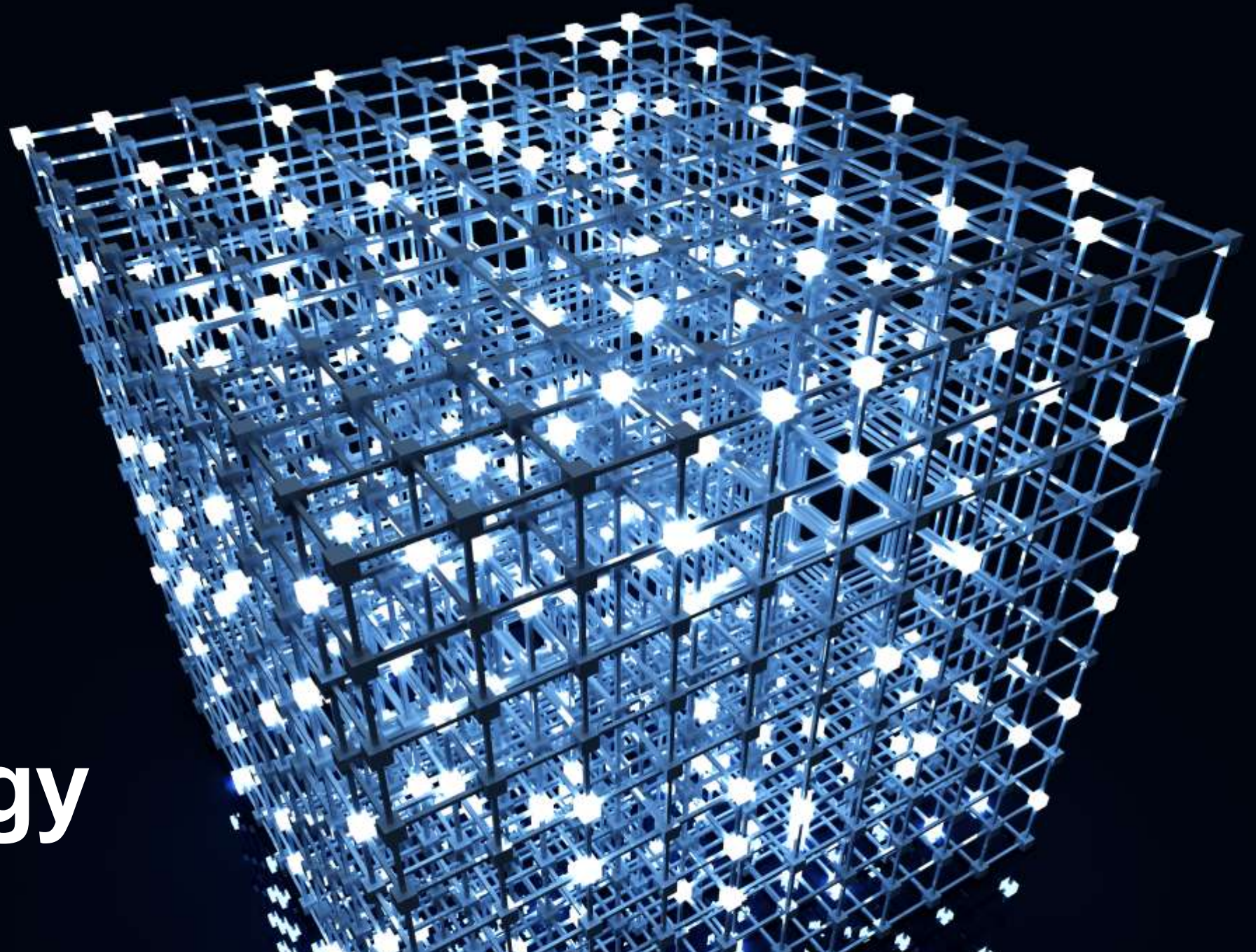
 **BROAD**
 **POWERFUL**
 **AUTOMATED**



BROAD

Deeper **visibility and control** throughout the Security Fabric
to reduce the attack surface from **IoT to Cloud**

Fabric Topology Views



Network Topologies

- Segmentation brings more complexity to network topologies.
 - » It becomes easy to make mistakes we can hardly see afterwards
 - » Congestions and bottlenecks get harder to locate



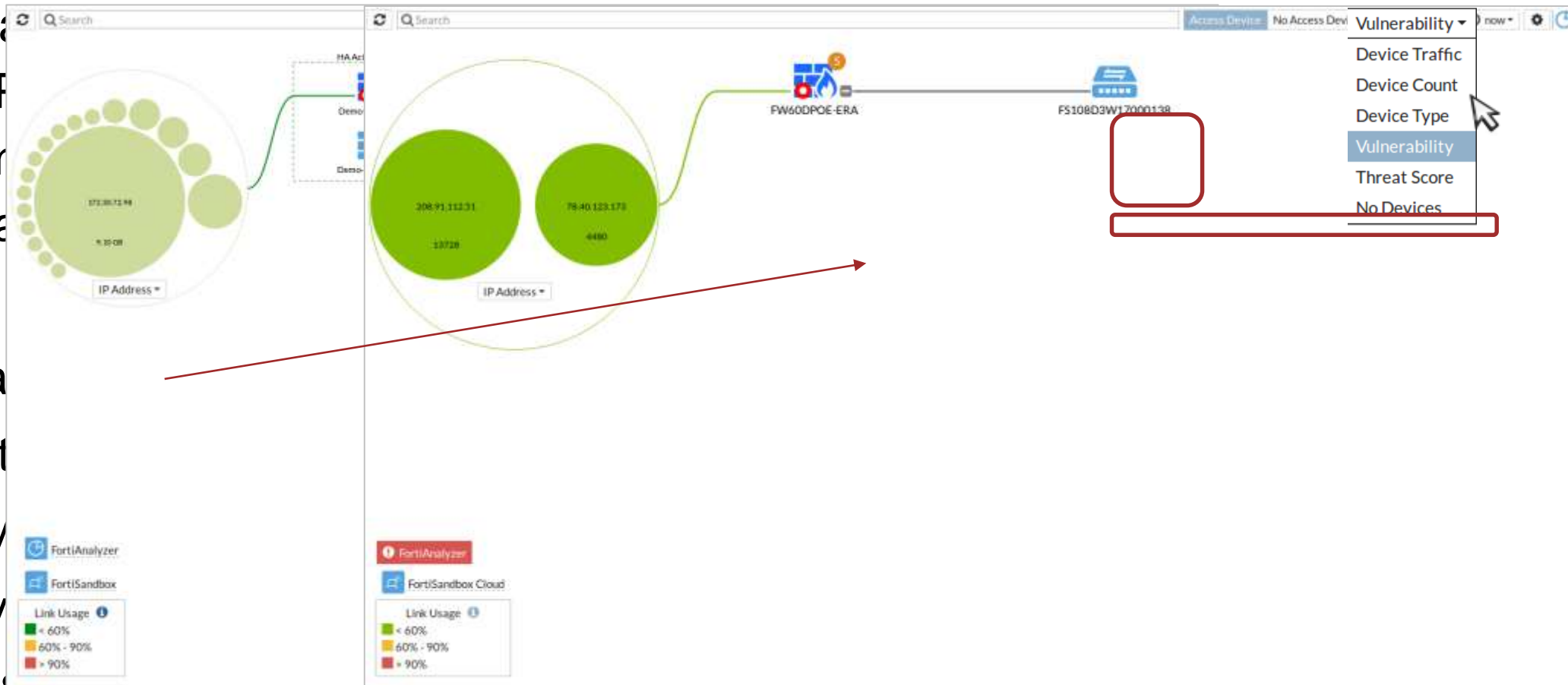
Fabric Topology View

- Fabric Topology Views are now added to 5.6

- » FortiGate
- » FortiAP
- » FortiAnalyzer
- » FortiSwitch

- Endpoint
- Links usage
- User avat
- OS & dev
- Rank dev

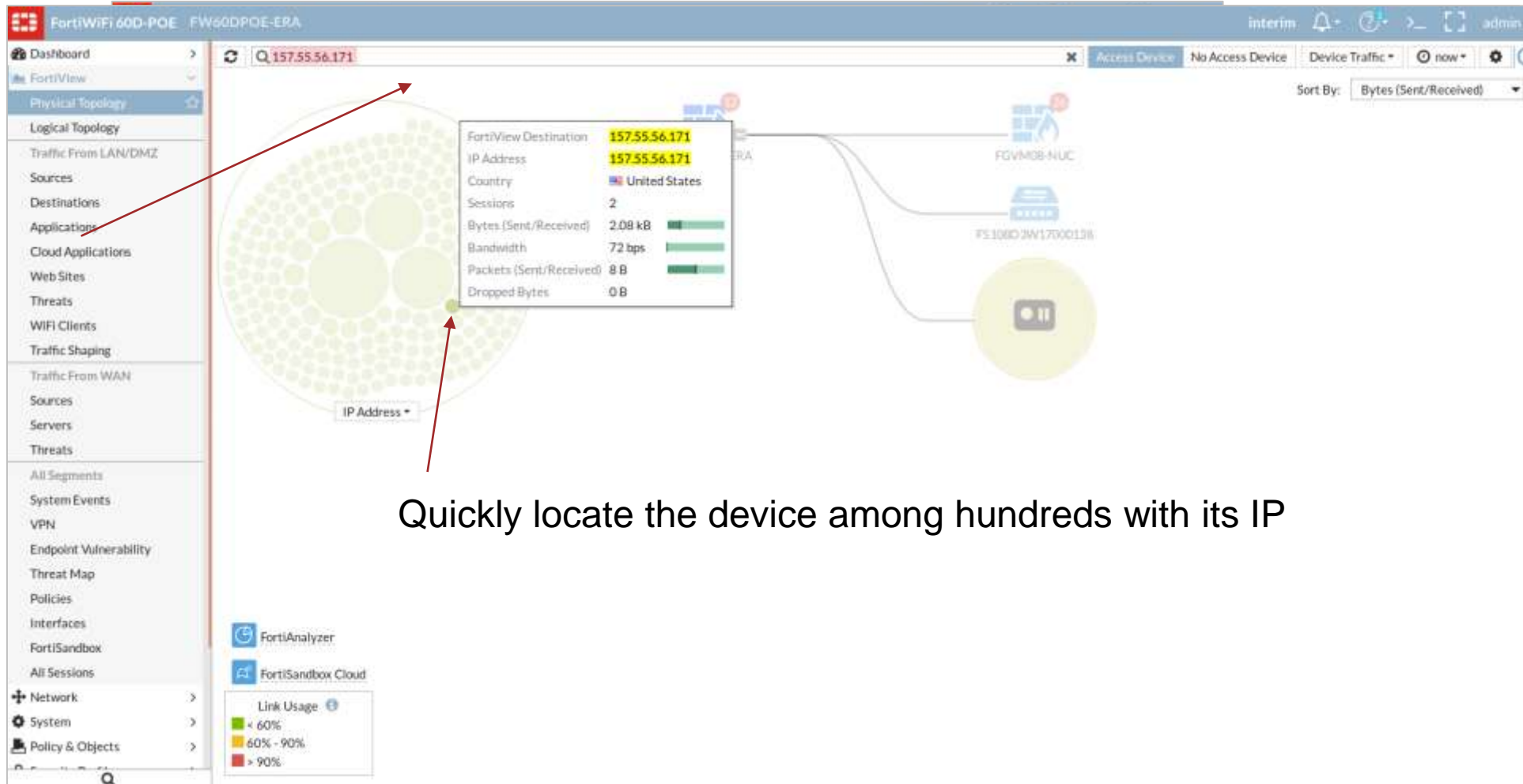
FortiClient score (bubble)



“Search” feature in topology

- Helps to quickly locate and size relevant information

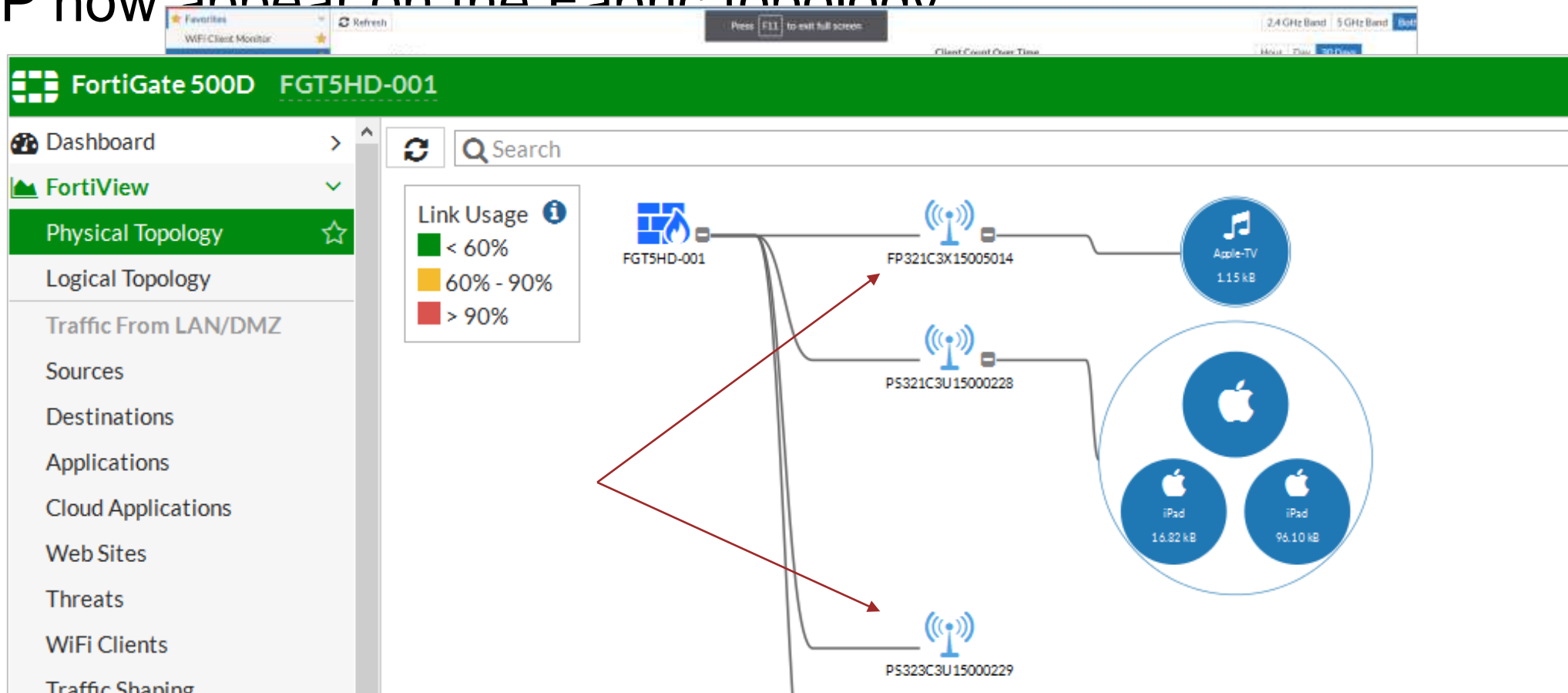
Search for
A specific
information
(device...)



Quickly locate the device among hundreds with its IP

Better visibility on wireless network

- New fortiview Wifi Health Monitoring
- AP now appear on the Fabric topology



Visibility on Endpoints Vulnerability

- Endpoints covered in the Security Fabric are ranked by their FortiClient

- » Visible on 'E
- » Score is calc
- » Supports dri

Endpoint: Win8-64-Test Add Filter

Summary of Win8-64-Test

User :	test (10.1.200.184)
Detected Vulnerabilities :	378
Time Period :	Last 24 Hours

Vulnerability Name	CVE-ID
Access violation with XSLT and uninitialized data	2013-5604
Arbitrary code execution within Profiler	2013-1688

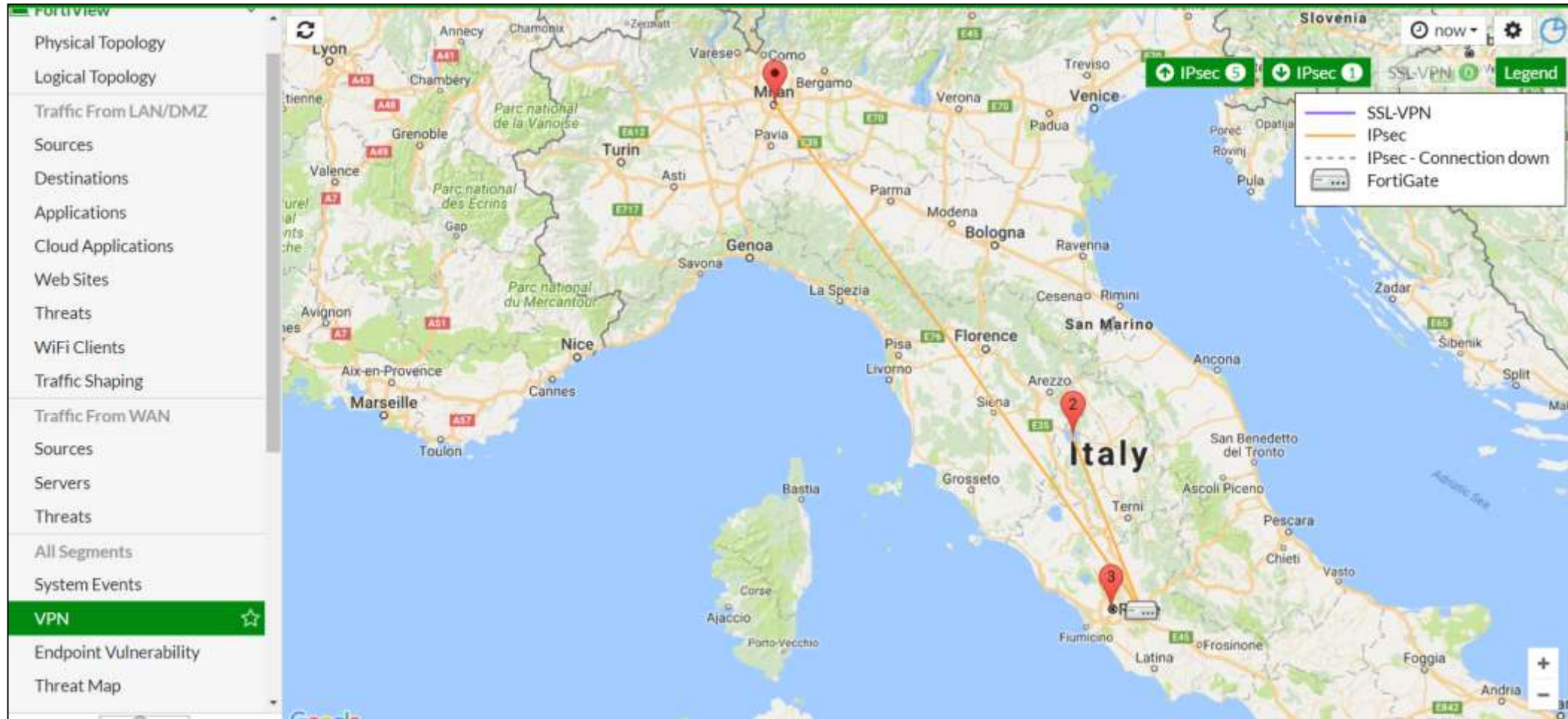
agentile
10.10.80.11

Device	mis-11YKP72	
Status	Registered	
Vulnerabilities	5 8 29 3	
MAC Address	84:7b:eb:23:71:fa	
Other MAC Addresses	b8:08:cf:29:2b:ba b8:08:cf:29:2b:bb b8:08:cf:29:2b:be	
Online Interfaces	LAN-Ufficio	
OS	Windows / 10	
Topology	FGT-FTNT-Roma mis-11YKP72	
Sessions	15	
Bytes (Sent/Received)	8.98 MB	
Bandwidth	2 kbps	
Packets (Sent/Received)	80.40 kB	
Dropped Bytes	0 B	

Demo – FortiView

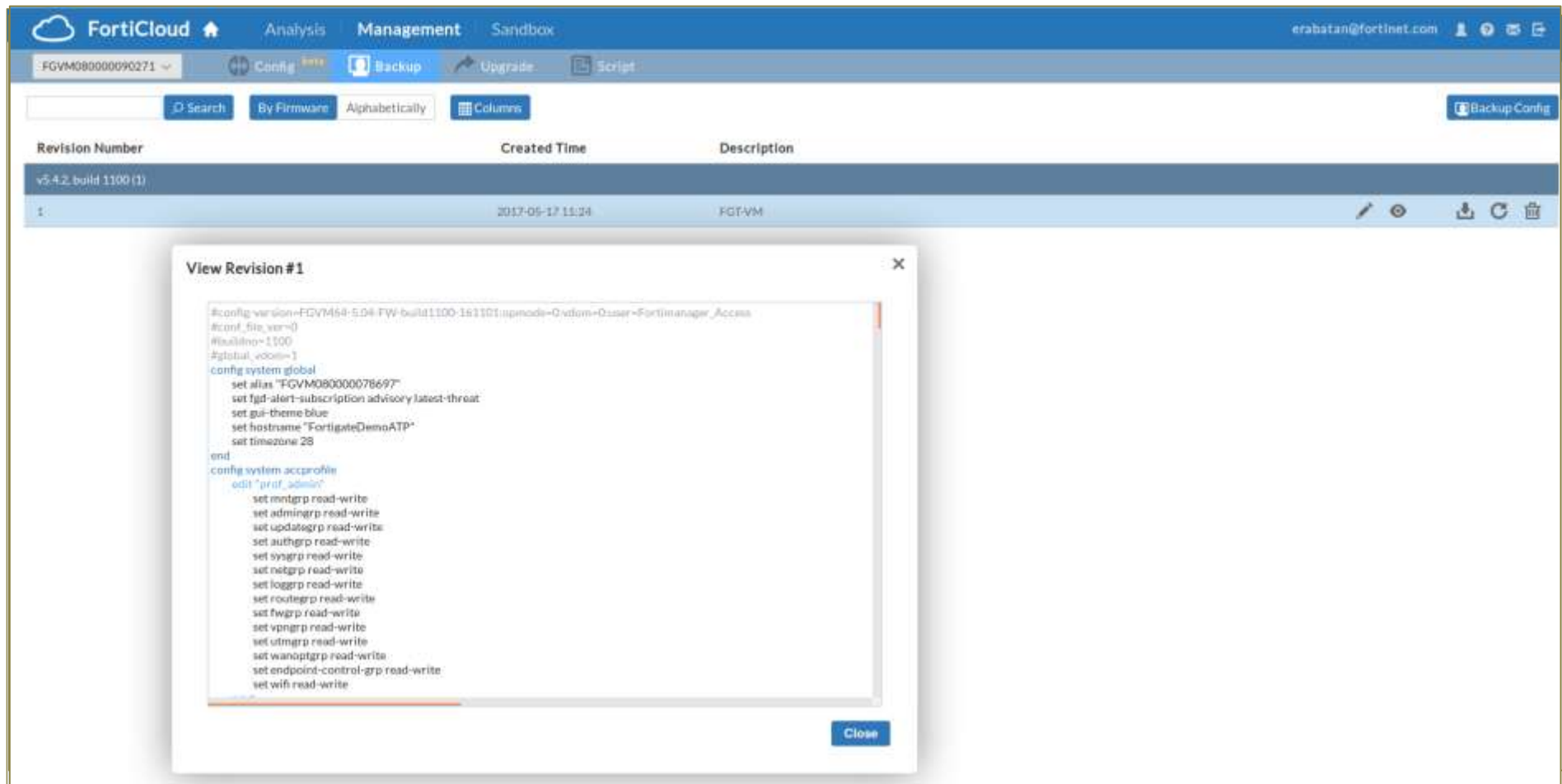
VPN tunnel map

- Help to materialize VPN tunnels on a map and quickly check their status



Central Visibility on Forticloud Fabric

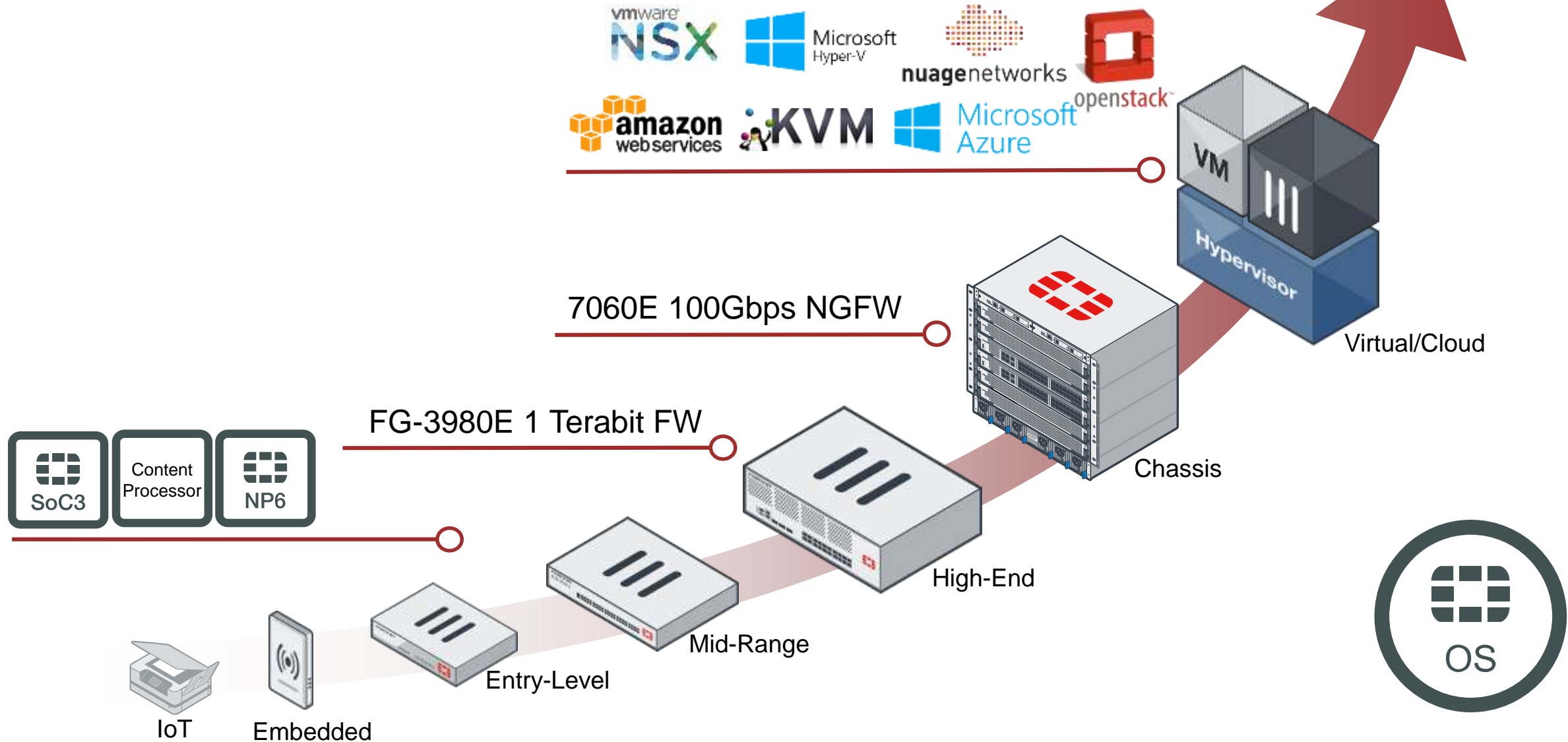
- All security components and virtual services available through one click



POWERFUL

Accelerated cloud-scale and security processor-based appliances with coordinated logging **to enable maximum threat protection without affecting performance**

Scaling Performance from IoT to Cloud

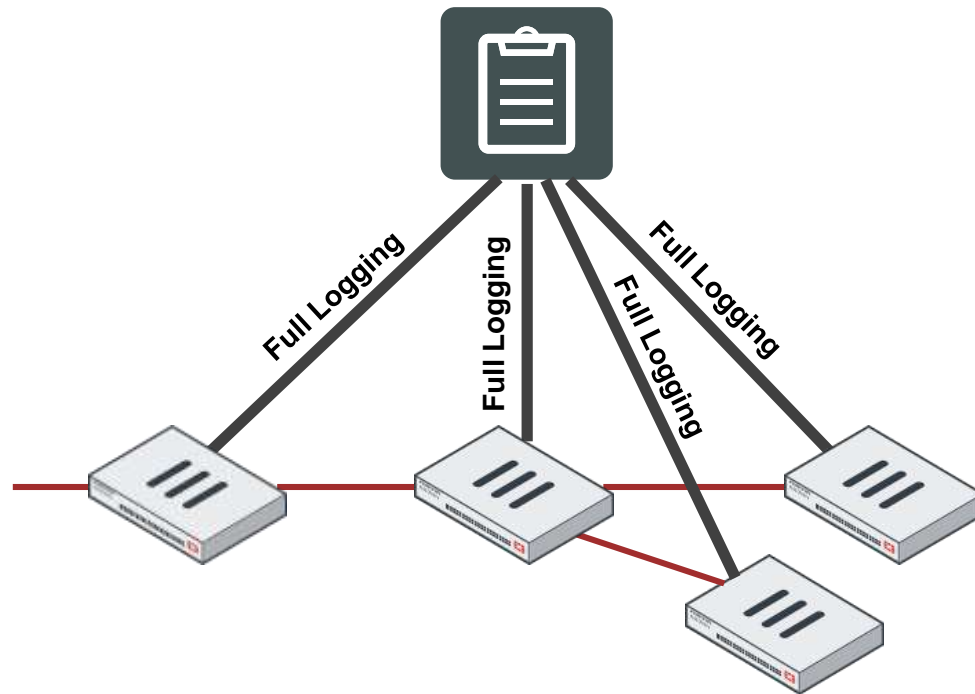


Hardware Acceleration

- NP6 Host protection engine
 - » Host protection against DDoS attacks at NP level
 - » CLI Option, apply to each NP6 processor separately
 - » User may set threshold based on each packet type (eg. TCP SYN) based on packet per second
- nTurbo (fastpath from external interfaces to IPS engine)
 - » Acceleration for sessions with flow-based security features
 - » Complete CP (pattern matching/pre-matching)

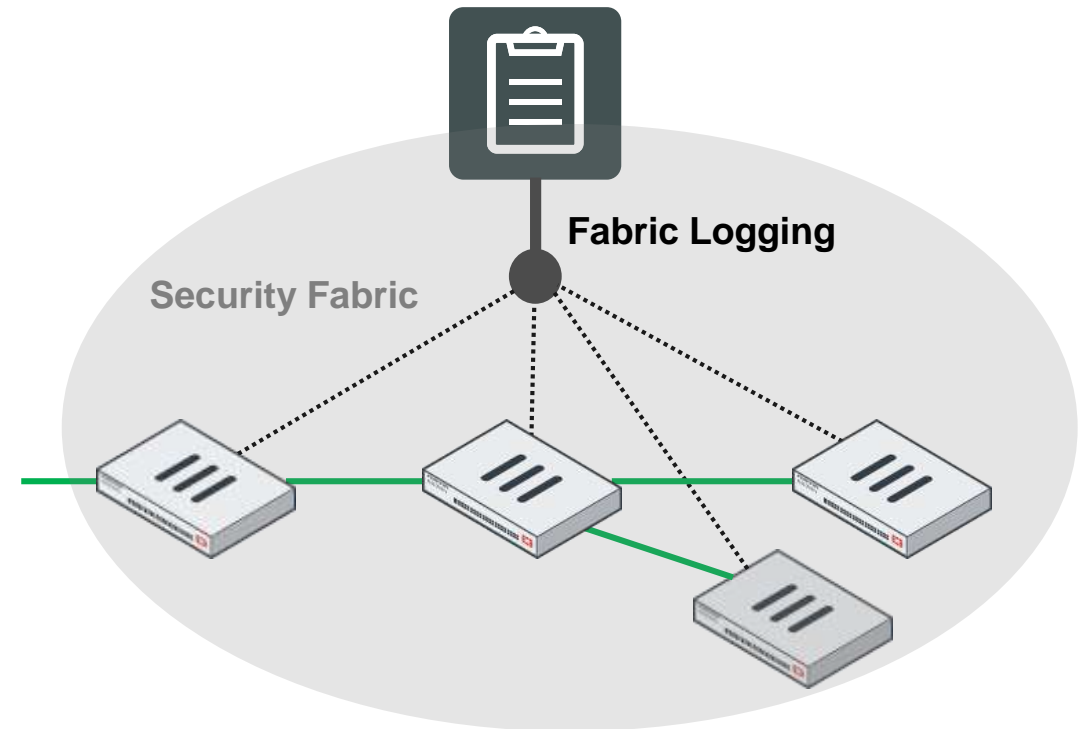
Coordinated Logging allows deep visibility and Better Performance

Uncoordinate



- Manual setting for each device for logging
- Each device sends full logging to FortiAnalyzer

Coordinated



- Automatic setting of all devices for logging
- Topology aware – log only what's needed

VM Enhancements

- Expand capacities and capabilities
 - » New VM with more vCPUs / memory up to 500 VDOMs
 - » VM08-UL support FortiOS Carrier Upgrade
 - » Number of virtual interfaces that FG-VM raises from 3 to 10
- Competitive pricing
 - » Cheaper VM option without VDOM capability for VM01 to VM04



NGFW Policy-based mode (1/2)

- Applications and/or URL categories can now be used as policy objects
 - » Requires flow-based mode and SSL insp.
 - » More flexible policy implementations
 - » Enables fall-through setups based on apps and web categories

Inspection Mode	Flow-based Proxy
NGFW Mode	Profile-based Policy-based
SSL/SSH Inspection	SSL certificate-inspection ▼

Name ⓘ	App Ctrl policy
Incoming Interface	port1 ✕
Outgoing Interface	port2 ✕
Source	all ✕
Destination	all ✕
Schedule	always ▼
Service	ALL ✕
Application	Google.Analytics ✕ Google.Business.Apps ✕ LucidChart ✕ LucidChart_File.Download ✕ Outlook.Anywhere ✕
URL Category	+ ✕
Action	✓ ACCEPT ✕ DENY ✕ LEARN ✕ IPsec

Name ⓘ	Block streaming websites
Incoming Interface	port1 ✕
Outgoing Interface	port2 ✕
Source	all ✕
Destination	all ✕
Schedule	always ▼
Service	ALL ✕
Application	+ ✕
URL Category	Streaming Media and Download ✕
Action	✓ ACCEPT ✕ DENY ✕ LEARN ✕ IPsec

NGFW Policy-based mode (2/2)

- Enables Central SNAT for the policies
- User must add Central SNAT policies

The screenshot shows the FortiGate web interface for configuring a new Central SNAT policy. The left sidebar contains navigation links: FortiView, Network, System, and Policy & Objects (selected). The main area is titled 'New Central SNAT Policy'. It features two input fields for interfaces: 'Incoming Interface' set to 'port2' and 'Outgoing Interface' set to 'port1'. Below these is a table listing the policy configuration.

Seq.#	From	To	Source Address	Destination Address	Translated Address	Original Port	Translated Port	Action
1	port2	port1	Internal	all				✓ PERMIT

Below the table, a sidebar on the left lists configuration options: Internet Service Database, Services, Schedules, Virtual IPs, IP Pools, Traffic Shapers, Traffic Shaping Policy, and Security Profiles. The main configuration area shows the 'NAT' toggle is enabled. Under 'IP Pool Configuration', 'Use Outgoing Interface Address' is selected. The 'Protocol' is set to 'ANY'. At the bottom, there are 'OK' and 'Cancel' buttons.



Security Audit

Security Fabric Audit

- Even the best tool can be misused
- Need assistance
 - » Mistakes
 - » Best practice
 - » Consistency
 - » ...



Security Fabric Audit

- Automates a full security audit on the configuration of the Fabric

Score

Policy	Last Used
all-internet	Never

Item	Policy	Last Used	Score	Action
Advanced Threat Protection	FW60DPOE-ERA		100	
Suspicious files should be submitted to FortiSandbox/FortiSandbox Cloud for inspection.	FOS-5-6-NUC		100	
Install a FortiSandbox and configure the FortiGate to send files to FortiSandbox for inspection. Alternatively, configure the FortiGate to send files to FortiSandbox Cloud.				
Unauthorized FortiSwitches	FW60DPOE-ERA		10	Easy Apply
All discovered FortiSwitches should be authorized or disabled.				
Authorize or disable the following FortiSwitches:				
• F5108D3W17000138				
Endpoint Compliance				
FortiClient Vulnerabilities	FOS-5-6-NUC		50	
All registered FortiClient devices should have no critical vulnerabilities.				
Have FortiClient fix the detected critical vulnerabilities on the following devices:				
WIN-KBED5G0QCQ				
Security Best Practices				
Detect Botnet Connections	FOS-5-6-NUC		100	
Interfaces which are classified as "WAN" should block or monitor outgoing connections to botnet sites.				
Block outgoing connections to botnet sites on the following interfaces:				
port1				
Replace the following devices with a FortiGate:				
34:e6:d7:82:67:16				
Third Party Router & NAT Devices	FW60DPOE-ERA		10	
No third party router or NAT devices should be detected in the network.				
Replace the following devices with a FortiGate:				
34:e6:d7:82:67:16				
Unsecure Protocol - Telnet	FOS-5-6-NUC		100	
Interfaces which are classified as "WAN" should not allow Telnet administrative access.				
Disable Telnet access on the following interfaces:				
port1				
Valid HTTPS Certificate - Administrative GUI	FW60DPOE-ERA		100	
The administrative GUI should not be using a default built-in certificate.				
Acquire a certificate for your domain, upload it, and configure the administrative GUI to use it.				
Explicit Interface Policies	FW60DPOE-ERA		5	
Policies that allow traffic should not be using the "any" interface.				
Change "any" to an explicit interface for the following IPv4 policies:				
• all-all				

< Back Next > Cancel

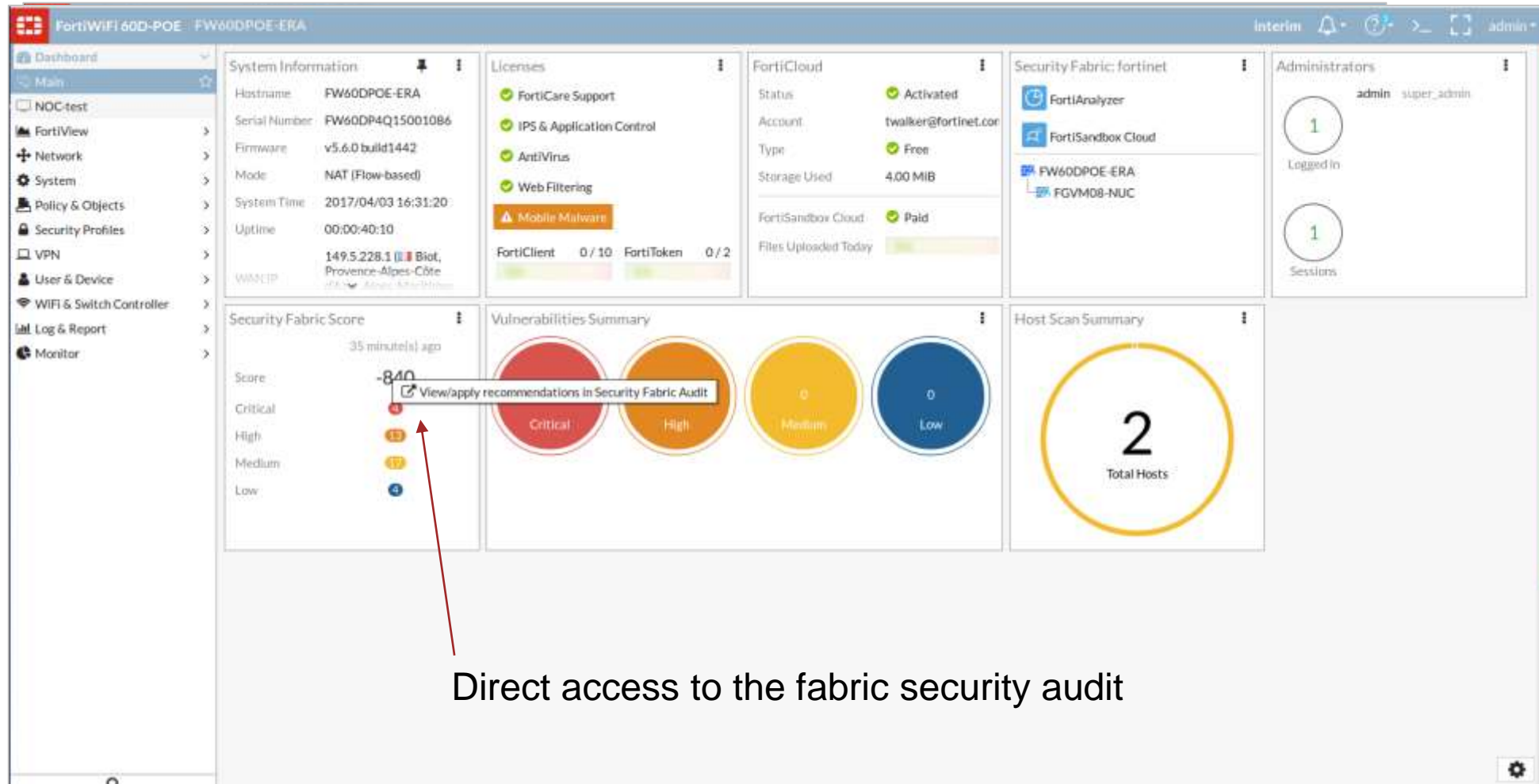
Easy Apply Only

Easy Apply

Select then make changes

New “Risk” widget from the Dashboard

- Risk widget provides the score for the security audit in a sec...



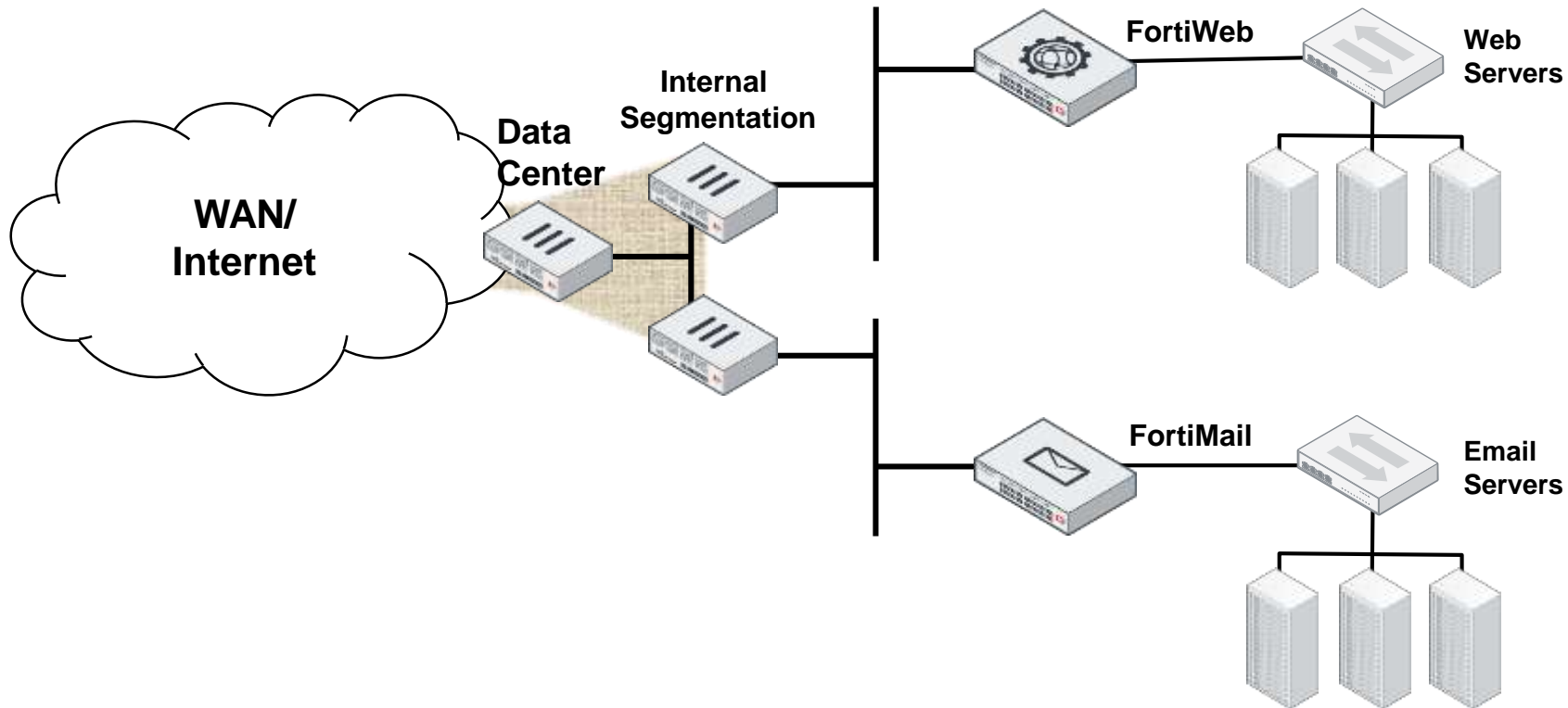
be resized

Demo – Security Fabric Audit

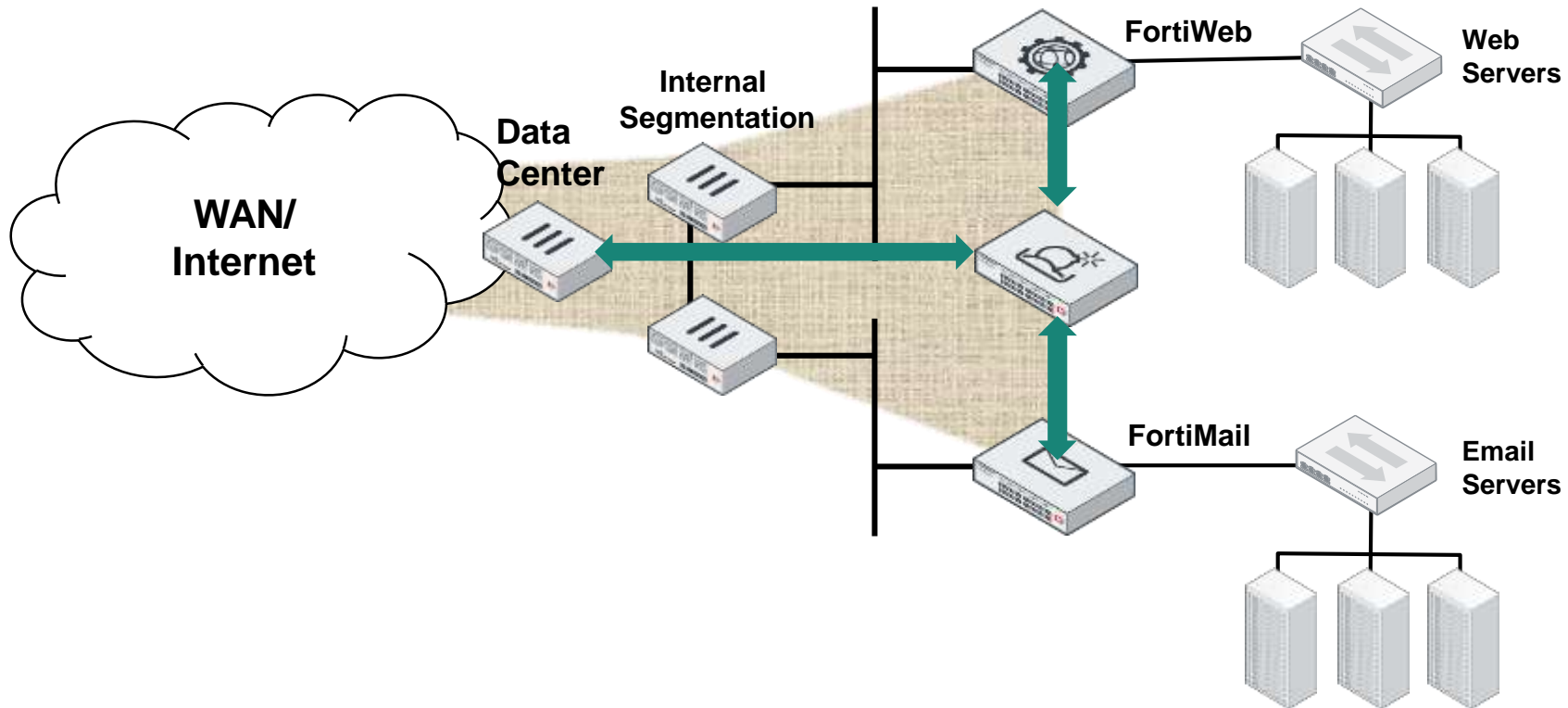
AUTOMATED

More efficient operations with new Security Fabric audit/recommendations, intelligence sharing, and NOC views

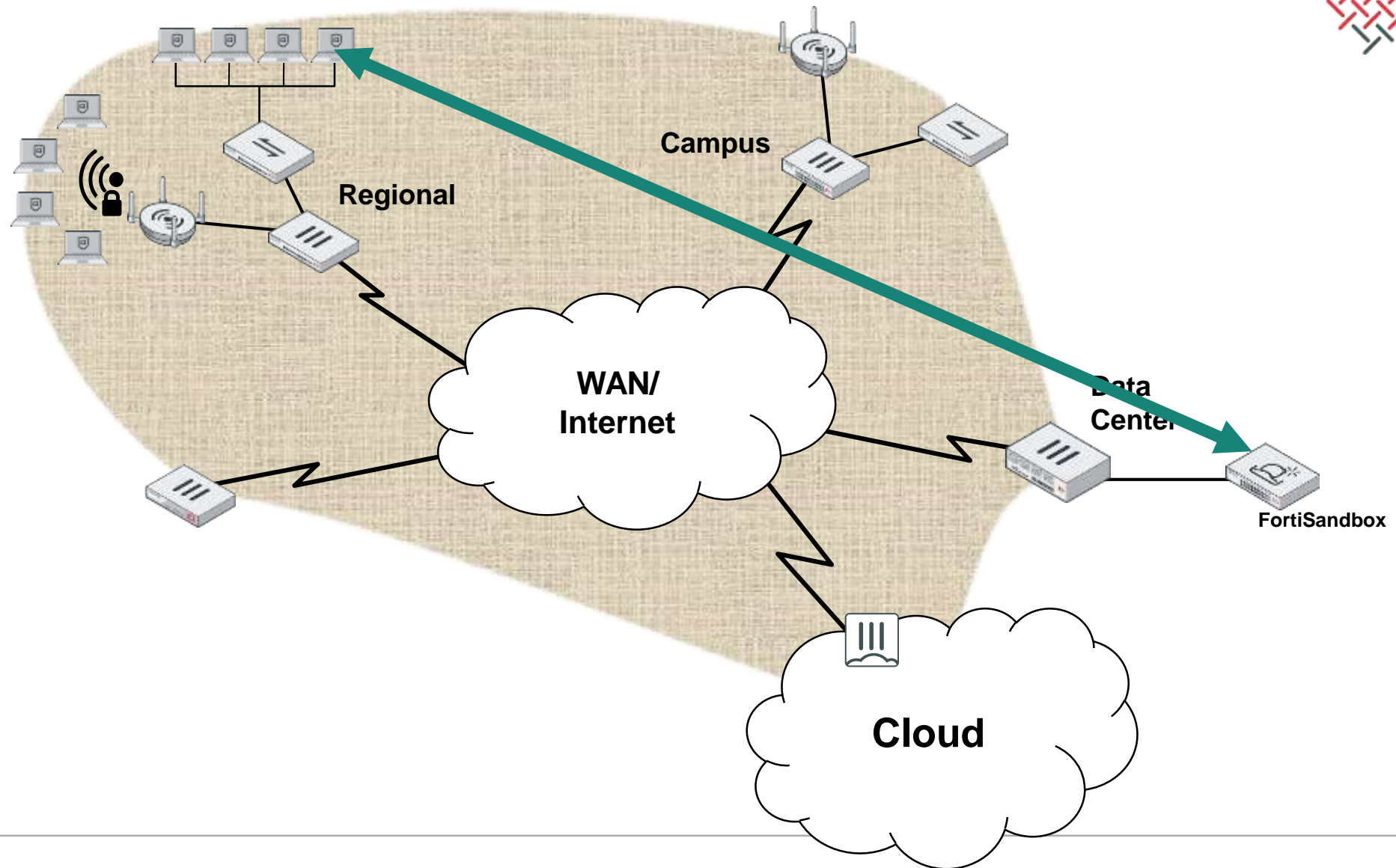
Meanwhile, Back in the Data Center...



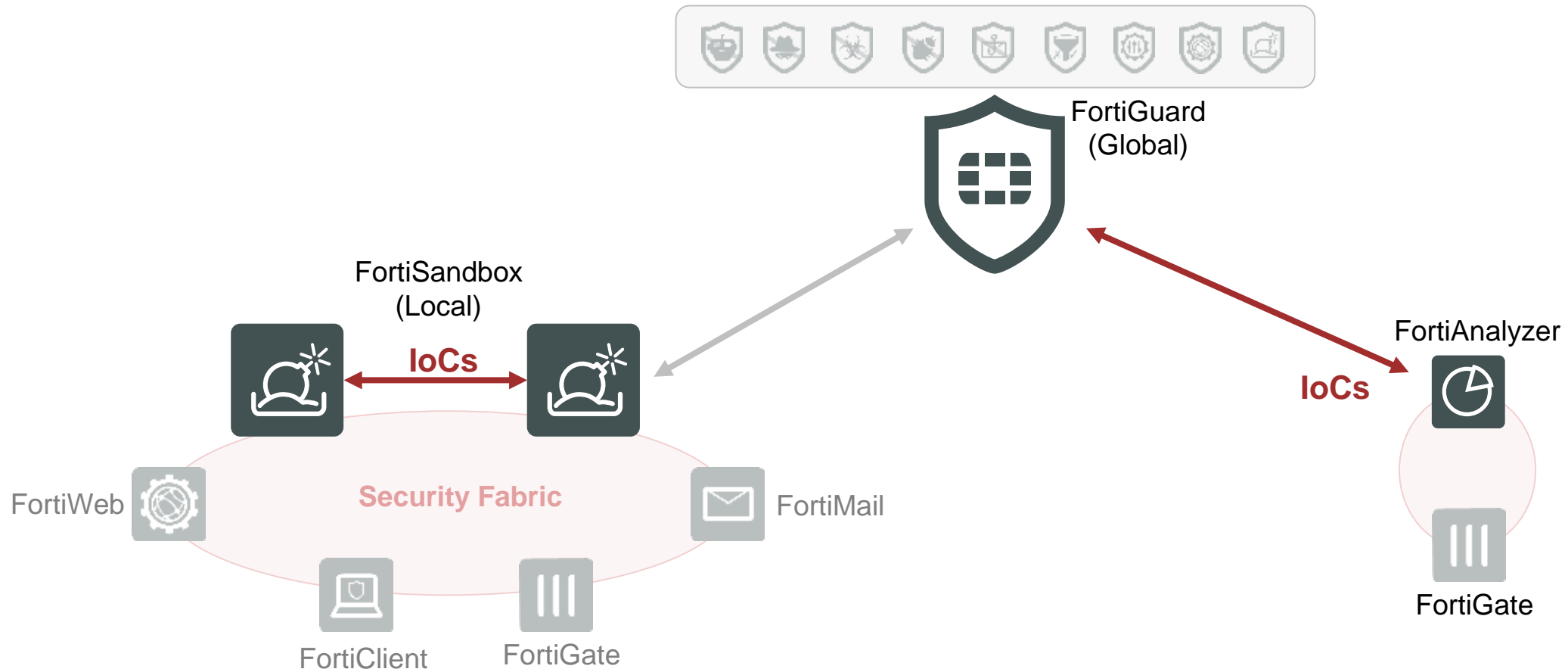
In the Data-Center



Extending Advanced Threat Protection to the Desktop



Rapid Sharing of Global and Local Threat Intelligence



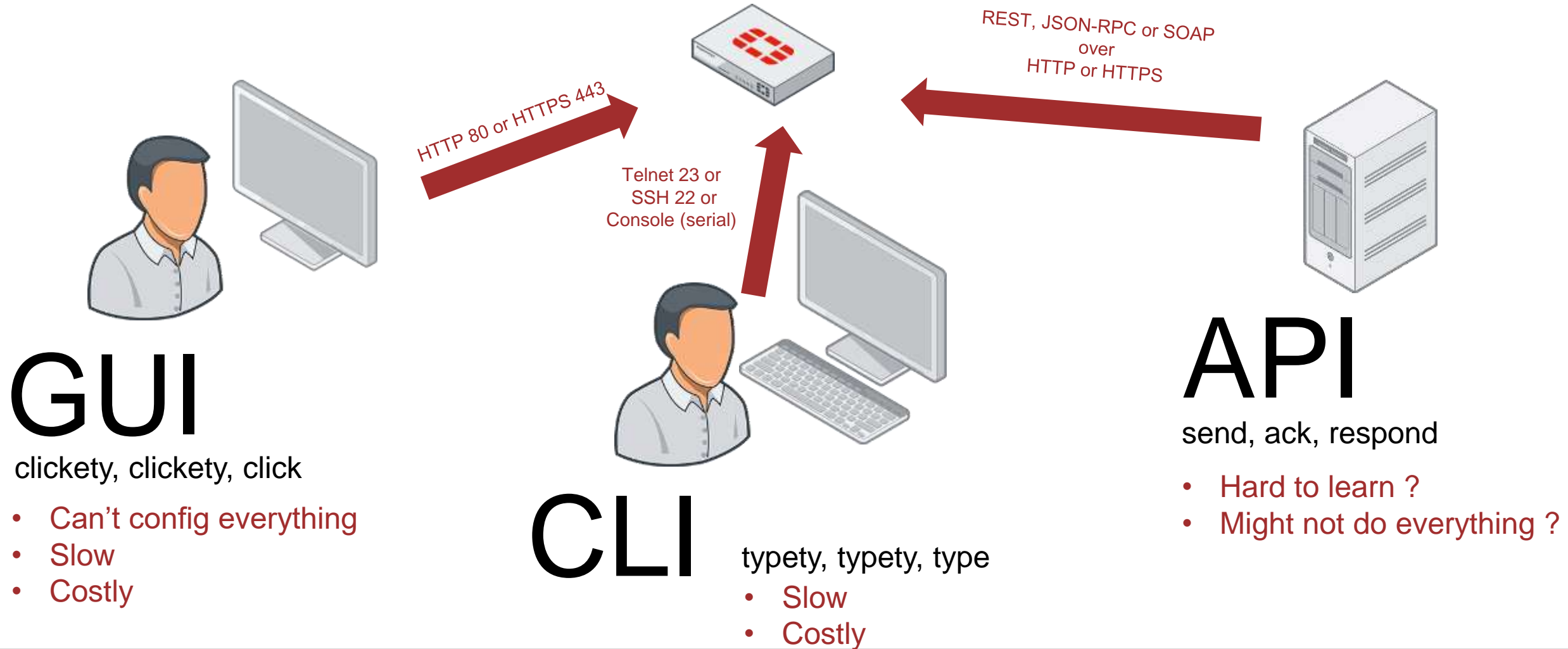
Clustered Local Intelligence distributed throughout the Security Fabric speeds mitigation

Correlation of Global IoCs and networking logs pinpoints new threats

Demo – Advanced Threat Prevention

What is an API?

API – Application Programming Interface “system talking to systems”



Which products have an API?



FortiGate



FortiManager



FortiAnalyzer



FortiSandbox



FortiAuthenticator



FortiWeb



FortiMail

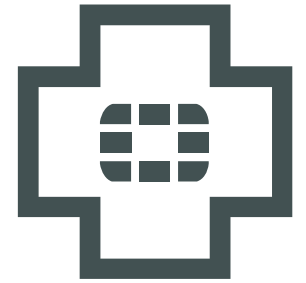


FortiDDoS

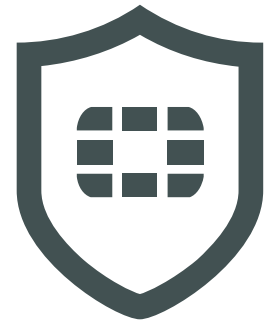


FortiCore

more



FortiCare



FortiGuard

The diagram illustrates the architecture of FortiManager for multi-tenant management, centered around the **MSSP FortiManager(s)** hub.

FortiGate CPE: Represented by a shield icon and a device icon. It interacts with the MSSP FortiManager(s) via **logs** and receives **Provisioning complete** notifications. It also receives **Device registers** and **Awaits instructions** from the MSSP FortiManager(s).

Customer SIEM: Represented by a server rack icon. It sends **CEF logs** to the MSSP FortiManager(s).

FortiAnalyzer: Represented by a clock icon. It receives **logs** from the FortiGate CPE and sends **REST/JSON** and **SOAP/XML** data to the MSSP FortiManager(s).

Customer Portal: Represented by a web interface icon. It sends **REST/JSON** data to the MSSP FortiManager(s). It also displays **Customer choices in customer portal sent via API** and a **Security Level Picker**.

Provisioning Server: Represented by a server rack icon. It receives **REST/JSON** and **SOAP/XML** data from the MSSP FortiManager(s) and applies templates based on user/svc class.

MSSP FortiManager(s): The central hub, represented by a clipboard icon. It manages the **Device DB** (represented by a cylinder icon) and **Policy Packages** (represented by a document icon).

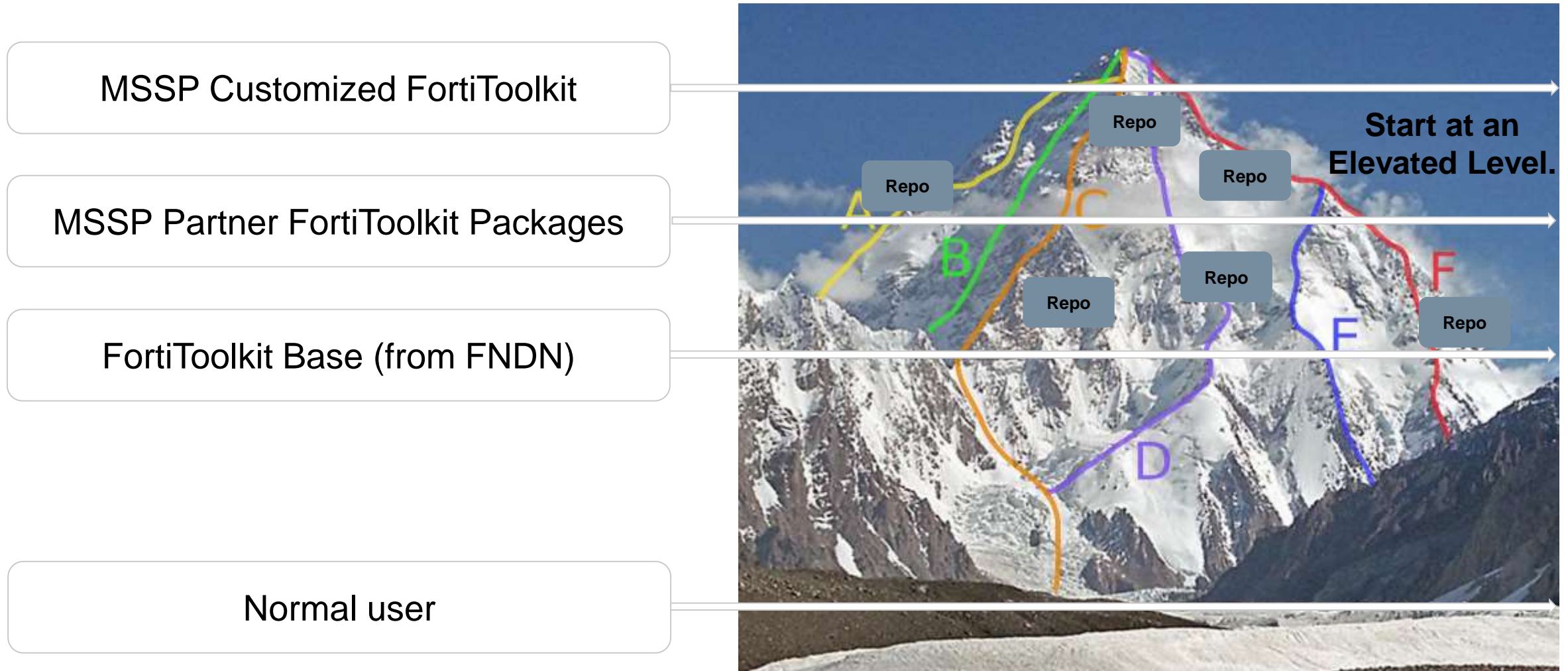
Key Features:

- Multi-tenant management
- Configuration repository / backups
- UTM/NGFW signature updates
- Firmware updates

Provisioning Process:

- Turns on device
- Device auto-provisions over LTE
- Optional wired network later; LTE becomes backup

Automation Jump Start - FortiToolkit



Security Fabric Beyond FortiWorld

Fortinet Reference Architecture

Advance Threat Protection (ATP) Framework

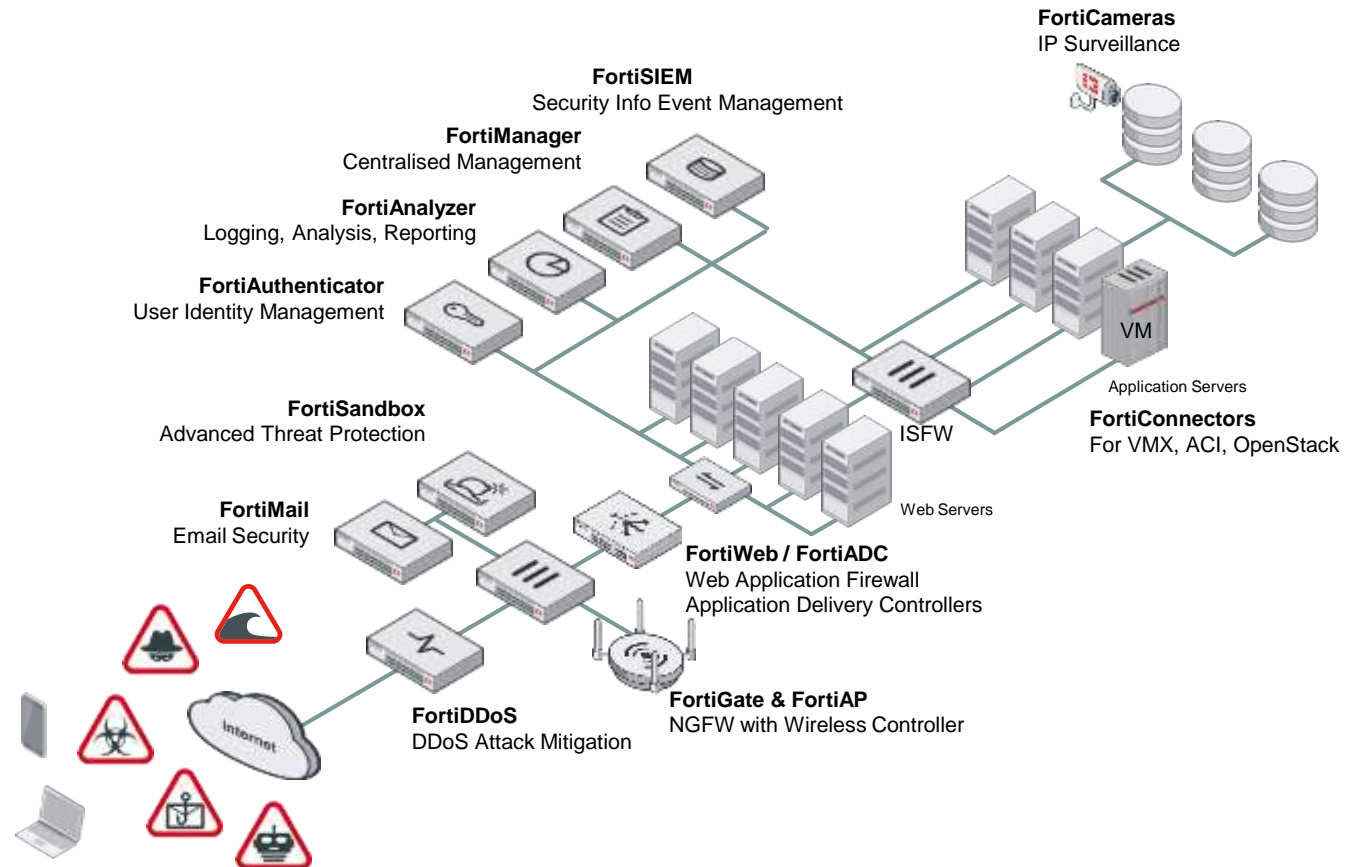


FortiToken
Two Factor Authentication

FortiClient
Endpoint Protection, VPN



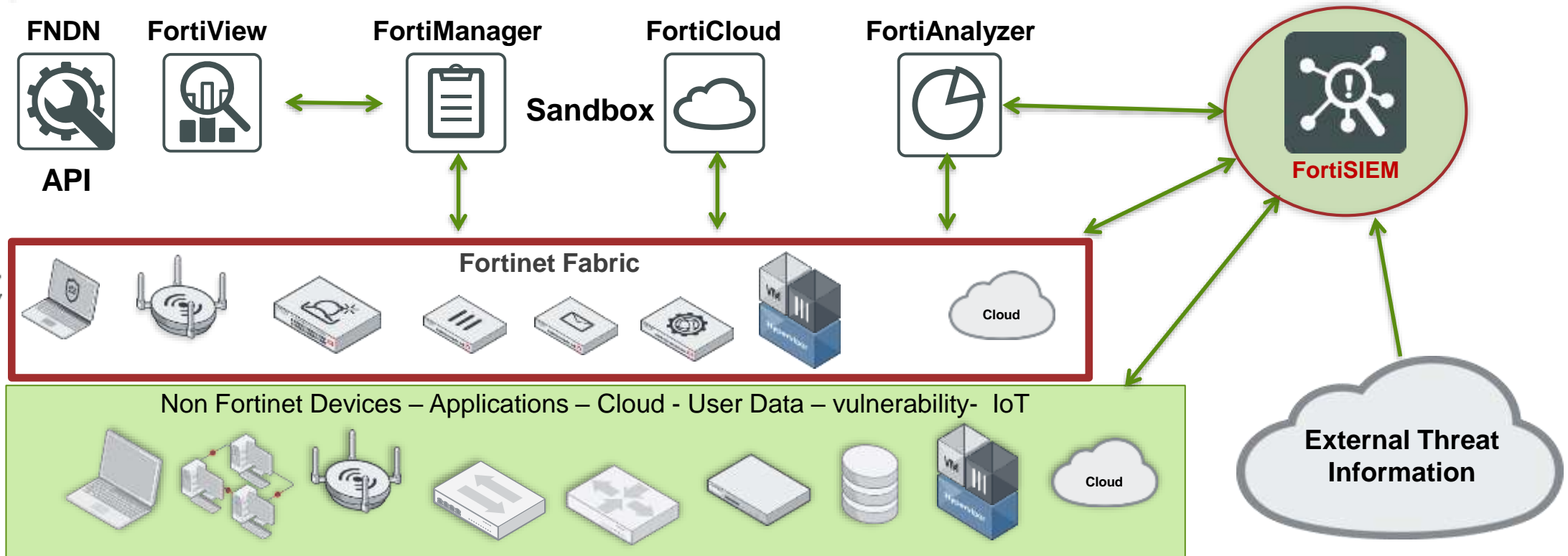
AWS & Azure
Fortinet Solutions
FortiCloud Analytics & Management



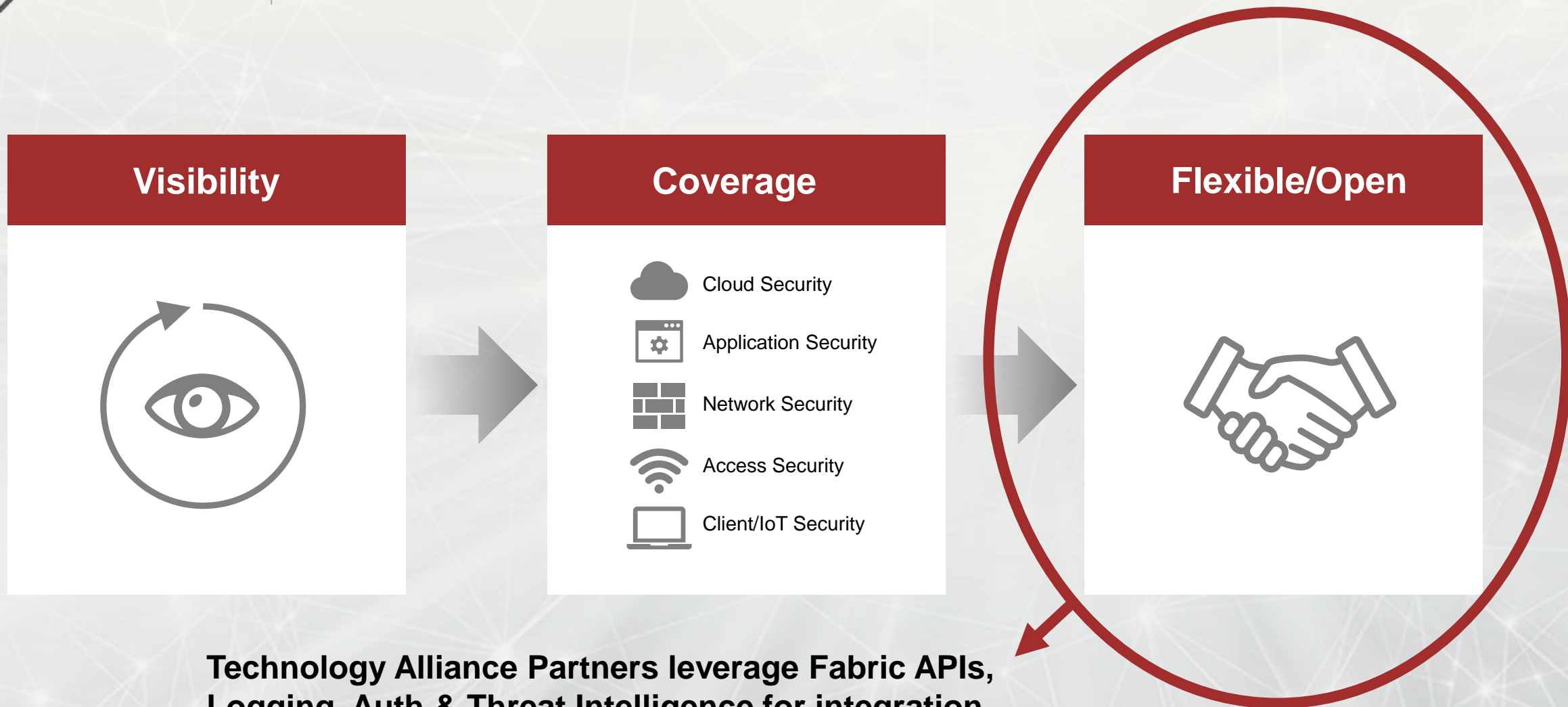
Secure by
FORTIGUARD™

Visibility Beyond Fortinet Products – FortiSIEM!

Integrated Security – Performance & Availability Monitoring



Broad – The Fabric Gives You Complete Visibility, Coverage and Flexibility Across The Entire Dynamic Attack Surface



Fortinet Fabric-Ready Partner Program

- Leverages Security Fabric APIs to deliver pre-integrated, end-to-end security offerings
- Integrated products improve threat awareness & intelligence, broaden & coordinate threat response and policy enforcement
- Faster time-to-deployment & reduced costs due to pre-validation of solutions
- Fabric-Ready Program is a Premium category of Fortinet's Technology Alliance Partnerships
- Alliance Partnerships web page:

<https://www.fortinet.com/partners/partnerships/alliance-partners.html>



Fortinet Security Fabric

Fabric-Ready Partner Program

Benefits for Channel Partners



- Deliver more effective, more responsive security solutions that leverage the collaborative power of the Fortinet Security Fabric
- Speed business outcomes with integrated ecosystem solutions that address customers' needs. Through Fabric-Ready pre-validation, gain access to more opportunities you can quickly sell into
- Leverage Fortinet's Fabric-Ready seal of approval to build trust with customers and instill confidence that the solutions work
- Deliver solutions with faster time-to-deployment to customers, with reduced technical support burden & costs due to pre-validation

Fortinet Technology Alliance Partnerships



Virtualization & SDN/NFV



CLOUD



ENDPOINT & IoT



MANAGEMENT



SIEM



SYSTEMS INTEGRATOR



Fabric-Ready Partners

Cisco

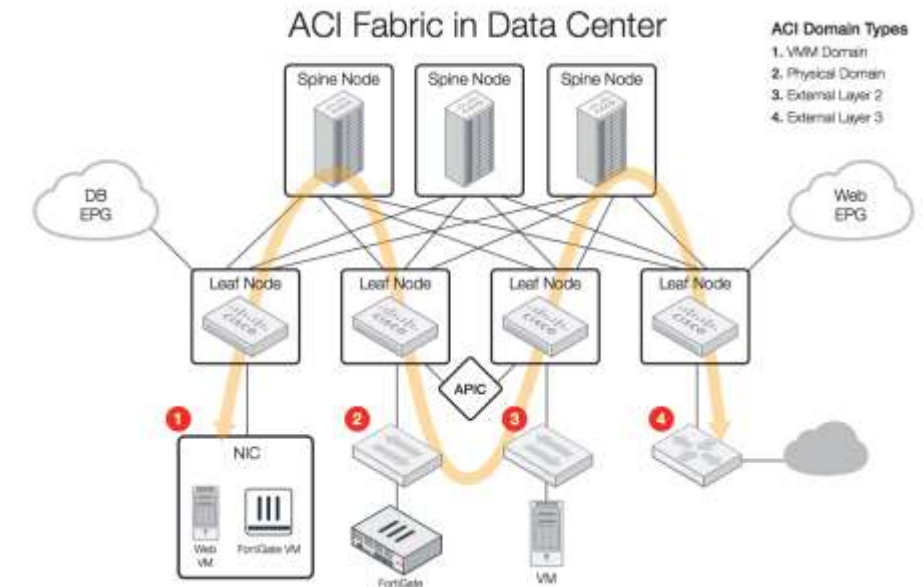
Key Solution Features

- The integration of Cisco ACI architecture with FortiGate provides automated, predefined policy-based security provisioning and security policy updates for NGFW, UTM and VPN services.
- Single-pane-of-glass management enablement from Cisco APIC with full visibility on security policy enforcement.
- Predefined security policies are deployed rapidly through complete application deployment lifecycle
- Consistency and transparency across physical and virtual application workloads, and scale on-demand with automation.

Key Benefits

- Better visibility and security correlated with overlay/underlay networks.
- Lower TCO from reduced administrative OPEX Accelerated application and L4-L7 security deployment.
- Increased efficiency in service provisioning and network security segmentation.

Integration: Virtualization & Management APIs



Fortinet-Cisco ACI Solution

Solution brief:

<https://www.fortinet.com/content/dam/fortinet/assets/alliances/Cisco-ACI-SolutionBrief.pdf>

Fabric-Ready Partners

Nozomi Networks



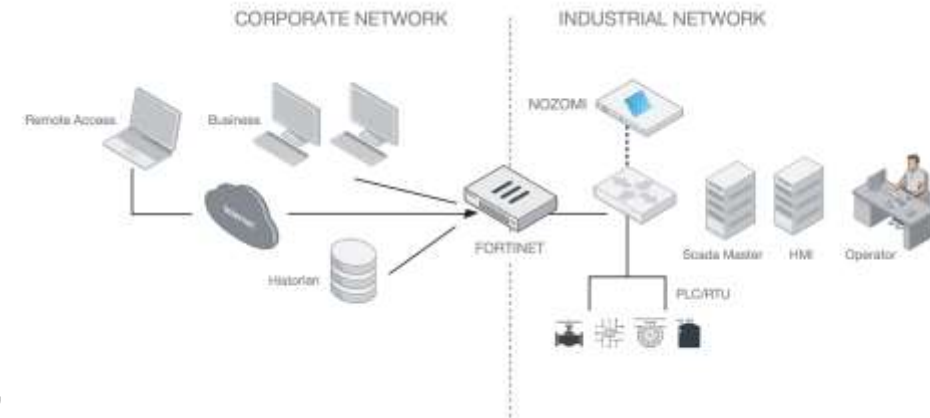
Key Solution Features

- Nozomi SCADAguardian implements innovative technology for monitoring and assessing Industrial Control Systems.
- Connects to the industrial network non-intrusively and in a fully passive mode, listening to all traffic between the control and field networks, analyzing it at all levels of the OSI stack (from L1 to L7).
- Uses Artificial Intelligence and Machine Learning techniques to create detailed behavior profiles for every device according to the process state, detecting critical states in the process.

Key Benefits

- Enhance security for ICS networks via sophisticated detection of ICS security issues with proactive threat remediation and containment.
- Reduce operational complexity and costs via centralized management, logging and reporting.
- Provides best-in-class visibility, security, monitoring, alerting, reporting, troubleshooting, and forensic capabilities.

Integration: Endpoint and Management APIs.



Fortinet-Nozomi Networks Solution for Securing Industrial Control Systems

Solution brief:

<https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Fortinet-Nozomi.pdf>

Fabric-Ready Partners

Qualys



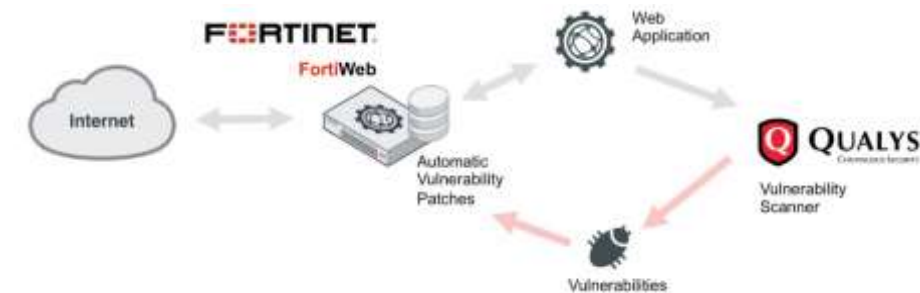
Key Solution Features

- Qualys Web Application Scanning (WAS) is a cloud service that provides automated crawling and testing of custom web applications to identify vulnerabilities including cross-site scripting (XSS) and SQL injection.
- The integrated solution that scans applications for vulnerabilities with Qualys WAS and protects them with Virtual Patching on the FortiWeb WAF. Once a vulnerability is discovered, it's protected by FortiWeb instead of issuing disruptive emergency patches.

Key Benefits

- Fewer disruptions due to emergency fixes and test cycles by virtually patching vulnerabilities until they can be permanently fixed.
- Reduced risk of exposure to threats between the time a threat is discovered until it is fixed by developers.
- Protection for legacy, inherited, and third-party applications where development fixes aren't an option or are impractical.

Integration: Management APIs.



Fortinet-Qualys Solution for Web Application Vulnerability Scanning and Virtual Patching

Solution brief:

<https://www.fortinet.com/content/dam/fortinet/assets/solution-guides/SB-Fortinet-Qualys.pdf>

Summary

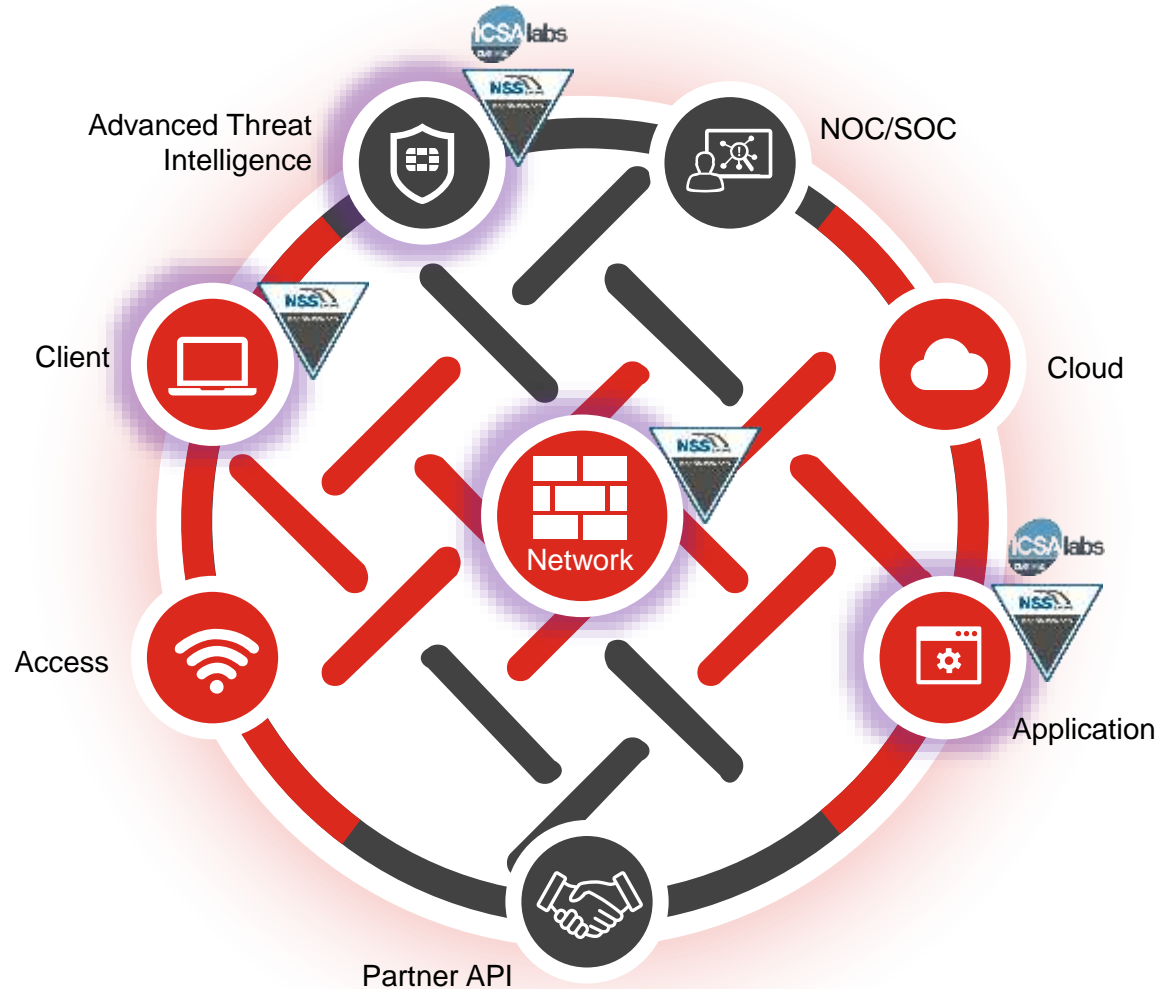
Let's keep some pieces!

What we have Covered in this Training

- Security Fabric Vision
 - Tight mesh of interconnected security controls
- Broad solution
 - Be informed about your environment, regardless what it looks like
 - Demo FortiView
- Powerful solution
 - Don't let security be an inhibitor, but an enabler
 - Security Fabric Audit demo
- Automated solution – profit to the max
 - Coordinated Advanced Threat Protection – demo
 - Go beyond FortiWorld



Only Vendor NSS Recommended At All Layers: Network, Application and Endpoint



- **Broad**
- **Powerful**
- **Automated**

The image features the FORTINET logo in white, bold, sans-serif capital letters. The logo is centered horizontally and slightly above the vertical midpoint. The background is a solid red color. Overlaid on the red background are several faint, white, stylized hexagonal patterns. These patterns consist of concentric hexagons and lines connecting the vertices of the hexagons, creating a network-like or molecular structure. The patterns are scattered across the image, with some being more prominent than others. The overall aesthetic is modern and technological.

FORTINET®